WITHCLUTCH

System and Organization Controls (SOC) 2 Type II

Report on Management's Description of

Clutch Platform

Report on Controls Placed in Operation and Test of Operating Effectiveness Relevant to the Trust Services Criteria for Security Category

For the Period
May 28, 2021 to November 30, 2021

Together with
Independent Service Auditor's Report

Table of Contents

I. Independent Service Auditor's Report

Johanson Group LLP Colorado Springs Colorado | San Jose California

Independent Service Auditor's Report

With Clutch, Inc.

Scope

We have examined With Clutch, Inc.'s accompanying description of its Clutch Platform (system) titled "Description of Clutch Platform" throughout the period May 28, 2021 to November 30, 2021 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria),* (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period May 28, 2021 to November 30, 2021, to provide reasonable assurance that With Clutch, Inc.'s service commitments and system requirements were achieved based on trust services criteria relevant to security principles (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

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

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at With Clutch, Inc., to achieve With Clutch, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents With Clutch, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of With Clutch, Inc.'s controls. 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 controls.

Service Organization's Responsibilities

With Clutch, Inc. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that With Clutch, Inc.'s service commitments and system requirements were achieved. With Clutch, Inc. has provided an assertion titled "Assertion of With Clutch, Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of the controls stated therein. With Clutch, Inc. is responsible for preparing the description and assertion; including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- 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 did not operate effectively.
- 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 controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements 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.

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 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 conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are presented in the section of our report titled "Description of Tests of Controls and Results Thereof."

Opinion

In our opinion, in all material respects,

a. The description presents With Clutch, Inc.'s Clutch Platform (system) that was designed and implemented throughout the period May 28, 2021 to November 30, 2021 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period May 28, 2021 to November 30, 2021, to provide reasonable assurance that With Clutch, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of With Clutch, Inc.'s controls throughout the period.
c. The controls stated in the description operated effectively throughout the period May 28, 2021 to November 30,2021, to provide reasonable assurance that With Clutch, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of With Clutch, Inc.'s controls operated effectively throughout the period.

Restricted Use

This report, including the description of tests of controls and results thereof in the section of our report titled "Description of Test of Controls and Results Thereof" is intended solely for the information and use of With Clutch, Inc.; user entities of With Clutch, Inc.'s Clutch Platform during some or all of the period May 28, 2021 to November 30, 2021, business partners of With Clutch, Inc. subject to risks arising from interactions with the With Clutch, Inc.'s processing system; practitioners providing services to such user entities and business partners; prospective user entities and business partners; 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, and 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 may affect the user entity's ability to effectively use the service organization's services.
- 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.

JohansonGroup LLP

Colorado Springs, Colorado
January 13, 2022

II. Assertion of With Clutch, Inc. Management

WITH**CLUTCH**

Assertion of With Clutch, Inc. Management

We have prepared the accompanying description of With Clutch, Inc.'s "Description of Clutch Platform" for the period May 28, 2021 to November 30, 2021, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)* (description criteria). The description is intended to provide report users with information about the With Clutch, Inc.'s Clutch Platform (system) that may be useful when assessing the risks arising from interactions with With Clutch, Inc.'s system, particularly information about system controls that With Clutch, Inc. 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 (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, (AICPA, Trust Services Criteria).*

With Clutch, Inc. uses a subservice organization to provide data center facility and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at With Clutch, Inc., to achieve With Clutch, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents With Clutch, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of With Clutch, Inc.'s controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at With Clutch, Inc., to achieve With Clutch, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents With Clutch, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of With Clutch, Inc.'s controls.

We confirm, to the best of our knowledge and belief, that:

a. The description presents With Clutch, Inc.'s Clutch Platform (system) that was designed and implemented throughout the period May 28, 2021 to November 30, 2021, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period May 28, 2021 to November 30, 2021, to provide reasonable assurance that With Clutch, Inc.'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 With Clutch, Inc.'s controls throughout that period.
c. The controls stated in the description operated effectively throughout the period May 28, 2021 to November 30, 2021, to provide reasonable assurance that With Clutch, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of With Clutch, Inc.'s controls operated effectively throughout that period.

With Clutch, Inc. Management
January 13, 2022

III. Description of Clutch Platform

Description of Clutch Platform

COMPANY OVERVIEW AND BACKGROUND

With Clutch, Inc. (“The Company”) was founded in Half Moon Bay in 2020 by Christopher Coleman and Nicholas Hinrichsen. After graduating from Stanford Business School in 2013, Christopher and Nicholas joined the startup accelerator YCombinator, raised Venture Capital in 2015, and eventually sold their first company to Carvana.com in 2017.

After spending 3 years at Carvana, the founders left in June 2020 to start The Company aiming to make car ownership more affordable. The Company provides APIs and loan application portals as a service (SaaS) to auto lenders and Credit Union.

The Company’s team is fully distributed, taking advantage of working with the best talent in the world without being limited to the Bay Area only. The team consists of people who amongst others worked at McKinsey, Bain & Company, Merrill Lynch, McLaren, Carvana, and NuBank with deep experience in digital auto retail and FinTech. The company is backed by Andreessen Horowitz, Peterson Partners, and a cadre of top-tier angel investors working amongst others at AirBnb, DoorDash, Asurion, and a number of other top tier technology companies

SERVICE PROVIDED

The loan portals allow lenders to turn demand for credit into ready-to-fund auto loans reducing the burden on both the borrower as well as the loan officer to an absolute minimum.

Hence, the portals make it incredibly easy to turn demand into ready-to-fund loan applications. At the same time, the APIs and services that are able to gather information from several sources drastically reduce the workload on loan officers creating efficiency gains and turning lenders into financial technology companies.

The services are a combination of a white label user experience and APIs. Once configured, the white label software will integrate with the lenders’ loan origination systems and lenders can start sending traffic to the portal.

A number of SaaS providers already have loan application user experiences in place. These clients usually leverage our APIs to enrich and enhance their existing experiences.

Both our portals as well as our APIs come with a robust analytics infrastructure. I.e. clients will have visibility into every step of the loan application process in real-time and via dashboards providing actionable guidance for business users.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

The Company designs its processes and procedures related to its platform to meet its objectives for a state-of-theart loan application process. Those objectives are based on the service commitments that the Company makes to user entities, the laws and regulations that govern the provision of credit services, and the financial, operational, and compliance requirements that the Company has established for the services. The loan application services of the Company are subject to the security and privacy requirements of state and local privacy security laws and regulations in the jurisdictions in which the Company operates.

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

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

- Security principles within the fundamental designs of the loan application platform are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

The Company establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in the Company's system policies and procedures, system design documentation, and contracts with customers.

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the loan application platform.

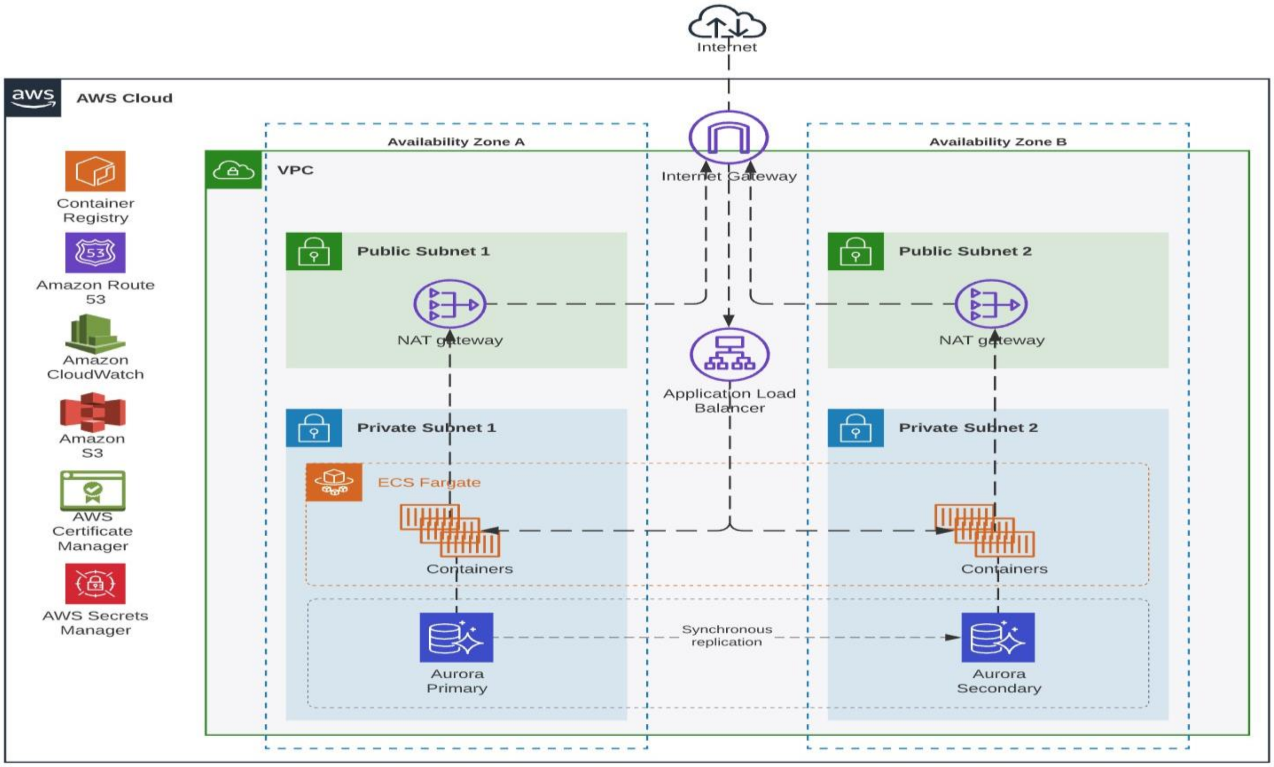
COMPONENTS OF THE SYSTEM

Infrastructure

The primary infrastructure used to provide the Company's loan portal includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
AWS	RDS	Database
AWS	ECS / Fargate	Elastic Container Service
AWS	EC2	Loan Balancer
AWS	Route 53	Routing
AWS	ACM	SSL Certificates
AWS	S3	File storage

Network Diagram



Software

The primary software used to provide the Company’s loan portal includes the following:

Primary Software	
Software	**Purpose**
GitHub	Version control and code management
PostgreSQL	Database
Node.JS	Backend code
React.JS	Frontend code
Google Analytics	Analytics
Nexmo	SMS identity verification
Sendgrid	Email gateway
Twilio	SMS gateway

People

The Company has a staff of 10 employees and contractors organized into 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.

- **Product Development**: Product managers and software engineers who design and maintain the loan portal product and APIs, including the web interface, the proprietary loan-to-vehicle matching engine, the window sticker tool, the loan payoff API, and all debugging tools. This team designs and implements new functionality assesses and remediates any issues or bugs found in the loan portal product and APIs, and architects and deploys the underlying cloud infrastructure on which the applications run. This team also implements new instances of the white label loan portal every time the Company signs up a new client. Members of the product team are responsible for peer reviews of code and infrastructure designed and authored within the team.

- **Product Operations**: The monitoring and maintenance of the loan portal product and APUs (once deployed) is handled by the operations role, which involves proactively designing and deploying monitoring software and tools to help identify errors or bugs in the loan portal product and APIs and remediate them either directly or via feedback to the product team. The operations team responds to alerts generated by our system, identifies issues with both loan portal and APIs and the configurations and SQL queries created by the Company's clients, and determines the best path to resolution. Operators also ensure that the loan portal is performing optimally (with high throughput and low latency) and that the loan portal is using the correct cloud infrastructure and scale to maintain high performance. Finally, operators are responsible for responding to any potential security issues with the loan portal and APIs and notifying affected clients if applicable.

- **Commercial**: Individuals with commercial roles work to market, sell, and support the Company's software. They are usually the primary point of contact to the Company's clients. They help identify which parts of the loan portal and APIs are most useful to prospective clients, and what new product development or new sync connections need to be engineered to meet customer needs. In the marketing role, the Company's employees identify best practices for automating business operations and provide that information to the Company's customers and prospective customers via webinars, blog posts, white papers, and other channels. Finally, the Company's client success team ensures that the Company's clients can use the product effectively and without errors, by assisting the Company's clients with onboarding into the product, helping identify useful data sources and author SQL models, and proactively identifying any issues or bugs that occur when users try to sync their data.

Data

There are three major types of data used by the Company:

- Configuration Data: Data used to configure the loan portals
- Customer Data: Data owned by the Company's clients that the loan portals load back and forth from the databases to the SaaS application
- Log Data: Logs, traces, and samples produced by the Company's engine while enabling the pre-client-configured Whitelabel portal

Configuration Data is stored in the Company's primary PostgreSQL databases and includes:

- The Company's clients' customers' data includes but is not limited to email addresses, names, physical addresses, birthdates, SSNs, etc.
- Credentials for accessing data warehouses, SaaS applications, and source code repositories, including usernames, passwords, OAuth tokens, and certificates
- The names of databases, schemata, tables, columns, custom objects, and custom fields in customers' databases and SaaS applications

- Configuration objects that determine how data is copied between systems, including field mappings, update policies, and schedules
- Audit logs covering changes to each of the above items

Configuration Data is treated as sensitive by the Company. It is stored with a limited lifetime when possible. Access controls limit configuration data access to each client's organization.

Customer Data is the most sensitive data in the Company's system. We attempt to limit handling and storing our clients' customer data to the extent possible:

- The Company's clients' customers data includes but is not limited to email addresses, phone numbers, names, physical addresses, birthdates, SSNs while SSNs are encrypted
- If our client has SSO technology available, we don't store our client's customer data in our database but instead request customer data in real-time and through the client's APIs.
- As described in our data retention and disposal policy, customer data is deleted upon termination of our contract with our client.

Log Data is produced by the loan portal to make it easier for the company's operators to monitor the health of the system and track down any issues. Log data is a trace of the actions performed by the system. Log data will include snapshots of Configuration Data at the time the loan application was used, so operators can see what the users of the loan portals were attempting to do. Log data also includes stack traces and samples of running code. Due to the nature of logging frameworks, there is a small possibility that log data can also include Customer Data captured by automatic tracers. The Company endeavors to "scrub" logs of any Customer Data before they are persisted. Log data may be stored by vendors that the Company has entrusted for purposes like indexing, monitoring, and trending. Regardless of whether log data is stored within the Company's own databases or by vendors, it is given a limited lifetime and automatically removed.

All data types processed by the Company and its applications are encrypted on the wire – no networking connections used by the Company for any purpose will ever send unencrypted data. In addition, all Configuration Data and Log Data, as well as samples of Customer Data stored by the Company is encrypted at rest, in our own databases, our caches, and our cloud storage.

PROCESSES AND PROCEDURES

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Company's policies and procedures that define how services should be delivered. These are located on the Company's intranet (i.e. within SecureFrame) and can be accessed by any of the Company's team members.

Physical Security

All data is hosted by Amazon Web Services (AWS). AWS data centers do not allow the Company's employees physical access. At present, the Company does not maintain any office space, and all work is conducted remotely.

Logical Access

The Company's employees and contractors are granted access to infrastructure via a role-based access control system, to ensure uniform, least-privilege access to identified users and to maintain simple and repeatable user provisioning and de-provisioning processes.

The Company's infrastructure runs entirely on cloud and SaaS-based systems, and as such the resources used by employees to perform their roles are accounts and permissions within those systems. An employee can have one of their access levels to a SaaS or cloud service:

- Administrator – can alter policies and provision or de-provision users
- User – has full read/write access to the SaaS or cloud service (except for administration)
- No access

Roles are reviewed on an annual basis by management and the security team to ensure least-privilege access.

The Company identifies employees primarily by their Okta account, which functions as our corporate directory and SSO provider. The Company's password policy mandates that employees and contractors use their Okta account to log in to their G Suite accounts to sign in to SaaS and cloud tools when supported. Employees authenticate themselves using a strong, unique password combined with an MFA authentication smart-phone app or 1Password integration.

The Company's Okta tenant requires users to use a second factor for authentication. In addition, any SaaS applications used by the company that doesn't use Okta or G Suite sign-in must be configured to use a second factor when possible.

The management team is responsible for onboarding new employees. Management is responsible for provisioning Okta, G Suite and other SaaS accounts as dictated by the employee's role and performing a background check, and the employee is responsible for reviewing the Company's policies, completing a security training, and successfully gaining access to provisioned accounts (as well as enrolling a device for second-factor authentication). These steps must be completed within 7 days of hire.

When an employee is terminated, management is responsible for removing or disabling all of the employee's accounts within 3 days.

The Company's employees may use a company-provided computer to perform their duties or may elect to "bring their own" device if that device is approved by the security team. Any computer (company-owned or BYOD) on which the Company's employee performs sensitive work must employ full-disk encryption and have an approved endpoint monitoring tool installed. On employee termination, management will ensure the return of company-owned devices and handle their deprovisioning or reprovisioning based on the company's Asset Management policy.

Computer Operations – Backups

Customer data is backed up by the Company’s operations team. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS, with physical access restricted according to applicable AWS policies. All backups are encrypted using KMS-managed encryption keys, with access restricted to key personnel via AWS IAM permissions.

Computer Operations – Availability

The Company maintains an Incident Response Policy that gives any Company-employee the ability to initiate a response to a potential security incident by notifying the internal security team through several channels and assisting in classifying the severity of the incident.

External parties (customers and third-party security researchers) are also given a channel to send encrypted incident reports and responsibly disclose potential issues to the Company’s security team.

Internally, the Company’s operations team monitors the health of all applications, including the loan application portals and APIs. Monitoring includes the availability and performance of the web UI, the throughput and queuing latency of the user experience, and any faults or errors encountered by users while configuring the loan portal. Critical incidents are routed to an on-call operator who is responsible for acknowledging within one hour; if there is no acknowledgment, the incident is escalated to the rest of the operations team.

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

Change Control

The Company 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.

Data Communications

The Company has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. Our PaaS simplifies our logical network configuration by providing an effective firewall around all the Company's application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

Our PaaS provider also automates the provisioning and de-provisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on the underlying hardware.

The Company uses GitHub to perform automated vulnerability scans after every deployment and engages an external security firm to perform semi-annual penetration testing to look for unidentified vulnerabilities, and the product engineering team responds to any issues identified via the regular incident response and change management process.

The Company does not maintain a corporate network, intranet, or VPN, but instead opts to use SaaS and cloud applications hosted on the public internet and secured by TLS connections.

BOUNDARIES OF THE SYSTEM

The scope of this report includes the Services performed by the Company. This report does not include the data center hosting services provided by AWS.

THE APPLICABLE TRUST SERVICES CRITERIA AND THE RELATED CONTROLS

Common Criteria (to the Security Category)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removals of information or system resources, misuse of the software, and improper access to or use of, alteration, destruction, or disclosure of information.

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 the Company's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of the Company'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.

Commitment to Competence

The Company'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 Company 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 our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way the Company 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 the Company 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 our 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 as a whole.

Organizational Structure and Assignment of Authority and Responsibility

The Company is currently organized in a simple, flat structure in which all employees report directly to the CEO. As the team grows, management will elect to build an organizational structure that ensures that employees clearly understand their role in the organization, how they and their team are responsible for furthering company-wide initiatives, and channels for reporting upward and downward in the organizational hierarchy.

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.

Human Resource Policies and Practices

The Company'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 ensures the service organization is operating at maximum efficiency. The Company's human resources policies and practices relating 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.

RISK ASSESSMENT PROCESS

The Company's risk assessment process identifies and manages risks that could potentially affect the Company's ability to provide reliable and secure services to our customers. As part of this process, the Company 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 re-evaluated annually, and tasks are incorporated into the regular Company product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of the

Company's system; as well as the nature of the components of the system result in risks that the criteria will not be met. The Company 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, The Company's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

INFORMATION AND COMMUNICATIONS SYSTEMS

Information and communication are an integral component of the Company'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.

The Company uses several information and communication channels internally to share information with management, employees, contractors, and customers. The Company uses chat systems (Slack) and email as the primary internal and external communications channels.

Structured data is communicated internally via our SaaS applications (finance information in our data warehouse and Stripe) and our project management tools (Linear). Finally, the Company uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

MONITORING CONTROLS

Management monitors control to ensure that they are operating as intended and that controls are modified as conditions change. The Company'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 is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

The Company's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon the 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 the Company's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing 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 the Company's personnel.

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of ongoing 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 IN THE LAST 12 MONTHS

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

INCIDENTS IN THE LAST 12 MONTHS

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

CRITERIA NOT APPLICABLE TO THE SYSTEM

All relevant trust services criteria were applicable to the Company Services system.

SUBSERVICE ORGANIZATIONS

The Company'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 the Company's services to be solely achieved by the Company's control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of the Company.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met.

Subservice Organization – AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	• Physical access to data centers is approved by an authorized individual.
		• Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		• Physical access to data centers is reviewed on a quarterly basis by the appropriate personnel.
		• Physical access points to server locations are recorded by a closed-circuit television camera (CCTV). Images are retained for 90 days unless limited by legal or contractual obligations.
		• Physical access points to server locations are managed by electronic access control devices.
		• Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

The Company management, along with the subservice organization, 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, the Company performs monitoring of the subservice organization controls, including the following procedures

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

The Company’s services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to the Company’s services to be solely achieved by the Company control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of the Company.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities’ locations, user entities’ auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to the Company.
2. User entities are responsible for notifying the Company of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of the Company services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize the Company's services.
6. User entities are responsible for providing the Company with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying the Company of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

IV. Description of Test of Controls and Results Thereof

Description of Test of Controls and Results Thereof

Relevant trust services criteria and With Clutch, Inc. related controls are an integral part of management's system description and are included in this section. Johanson Group LLP performed testing to determine if With Clutch, Inc.’s controls were suitably designed and operating effectively to achieve the specified criteria for the security category set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria),* throughout the period May 28, 2021 to November 30, 2021.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of With Clutch, Inc. activities and operations and inspection of With Clutch, Inc. documents and records. The results of those tests were considered in the planning, the nature, timing and extent of Johanson LLP's testing of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all With Clutch, Inc. controls, this test was not listed individually for every control in the tables below.

Trust Services Criteria for the Security Category	*Description of With Clutch, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
Control Environment			
CC 1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	With Clutch, Inc. has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of non-compliance. In addition, internal personnel acknowledges the Code of Conduct promptly on hire.	Inspected the company's Code of Conduct Policy and list of current employees to determine that the policy is in place outlining ethical expectations, behavior standards, and ramifications of non-compliance, and internal personnel acknowledges the Code of Conduct promptly on hire.	No exceptions noted.
	With Clutch, Inc. evaluates the performance of internal personnel through a formal, annual performance evaluation.	Inspected a sample of personnel's evaluation to determine that the company conducts these performance evaluations annually.	No exceptions noted.
CC 1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The board of directors or equivalent entity function includes senior management and external advisors, who are independent from the company's operations.	Inspected the company's list of the board of directors or any equivalent entity function to determine that it includes senior management and external advisors, who are independent of the company's operations.	No exceptions noted.
	Senior management and/or BOD meets at least annually to review business objectives, company initiatives, resource needs, and risk management activities.	Inspected the company's list of the board of directors or any equivalent entity function, and meeting minutes to determine that they meet at least annually to review business objectives, company initiatives, resource needs, and risk management activities.	No exceptions noted.
CC 1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Management maintains a formal organizational chart to identify positions of authority and the lines of communication and publishes the	Inspected company records to determine that management maintains a formal organizational chart to identify positions of authority and the lines of communication and publishes the organizational chart to internal personnel.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of With Clutch, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	organizational chart to internal personnel.		
	Management publishes the Acceptable Use policy to internal personnel. In addition, internal personnel acknowledges these procedures within 60 days of hire.	Inspected the company's Acceptable Use Policy and list of current employees to determine that management publishes the policy to internal personnel, and in addition, internal personnel acknowledges these procedures within 60 days on hire.	No exceptions noted.
	Management publishes the Data Classification Policy to internal personnel. In addition, internal personnel acknowledges these procedures within 60 days of hire.	Inspected the company's Data Classification Policy and list of current employees to determine that management publishes the policy to internal personnel, and in addition, internal personnel acknowledges these procedures within 60 days on hire.	No exceptions noted.
	Management publishes the Information Security Policy to internal personnel. In addition, internal personnel acknowledges these procedures within 60 days of hire.	Inspected the company's Information Security Policy and list of current employees to determine that management publishes the policy to internal personnel, and in addition, internal personnel acknowledges these procedures within 60 days on hire.	No exceptions noted.
CC 1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	With Clutch, Inc. has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of non-compliance. In addition, internal personnel acknowledges the Code of Conduct promptly on hire.	Inspected the company's Code of Conduct Policy and list of current employees to determine that the policy is in place outlining ethical expectations, behavior standards, and ramifications of non-compliance, and internal personnel acknowledges the Code of Conduct promptly on hire.	No exceptions noted.
	With Clutch, Inc. evaluates the performance of internal personnel through a formal, annual performance evaluation.	Inspected a sample of personnel's evaluation to determine that the company conducts these performance evaluations annually.	No exceptions noted.
	Background checks are performed on new hires before the new hire's start date as permitted by local laws.	Inspected the list of current employees to determine that background checks are performed on new hires before the new hire's start date as permitted by local laws.	No exceptions noted.
	Hiring managers screen new hires or internal transfers to assess their qualifications, experience, and competency to fulfill their responsibilities.	Inspected the review of resumes to determine that hiring managers screen new hires or internal transfers to assess their qualifications, experience, and competency to fulfill their responsibilities.	No exceptions noted.
	Internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security, availability, and confidentiality.	Inspected the list of current employees to determine that internal personnel complete annual training programs for information security, to help them understand their obligations and responsibilities related to security, availability, and confidentiality.	No exceptions noted.
	Management publishes the Acceptable Use policy to internal personnel. In addition,	Inspected the company's Acceptable Use Policy and list of current employees to determine that management publishes the	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of With Clutch, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	internal personnel acknowledges these procedures within 60 days of hire.	policy to internal personnel, and in addition, internal personnel acknowledges these procedures within 60 days on hire.	
	Management publishes the Data Classification Policy to internal personnel. In addition, internal personnel acknowledges these procedures within 60 days of hire.	Inspected the company's Data Classification Policy and list of current employees to determine that management publishes the policy to internal personnel, and in addition, internal personnel acknowledges these procedures within 60 days on hire.	No exceptions noted.
	Management publishes the Information Security Policy to internal personnel. In addition, internal personnel acknowledges these procedures within 60 days of hire.	Inspected the company's Information Security Policy and list of current employees to determine that management publishes the policy to internal personnel, and in addition, internal personnel acknowledges these procedures within 60 days on hire.	No exceptions noted.
CC 1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	With Clutch, Inc. evaluates the performance of internal personnel through a formal, annual performance evaluation.	Inspected a sample of personnel's evaluation to determine that the company conducts these performance evaluations annually.	No exceptions noted.
	Management maintains a formal organizational chart to identify positions of authority and the lines of communication and publishes the organizational chart to internal personnel.	Inspected company records to determine that management maintains a formal organizational chart to identify positions of authority and the lines of communication and publishes the organizational chart to internal personnel.	No exceptions noted.
	Violations of With Clutch, Inc. policies are subject to disciplinary action and such disciplinary action is documented in one or more policies.	Inspected the company's Information Security Policy to determine that violations of policies are subject to disciplinary action and such disciplinary action is documented in one or more policies.	No exceptions noted.
Communication and Information			
CC 2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	With Clutch, Inc. has a continuous monitoring solution for internal controls used in the achievement of the Company’s service commitments and system requirements.	Inspected the company's infrastructure and version control tool to determine that they have a continuous monitoring solution for internal controls used in the achievement of the Company’s service commitments and system requirements.	No exceptions noted.
	With Clutch, Inc. performs a formal risk assessment, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected company's records to determine that they perform a formal risk assessment, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No exceptions noted.
	Vulnerability scanning is performed on production infrastructure systems. With	Inspected company records to determine that vulnerability scanning is performed on production infrastructure systems. The	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of With Clutch, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	Clutch, Inc. remediates identified deficiencies on a timely basis.	company remediates identified deficiencies on a timely basis.	
	With Clutch, Inc. engages a third party to conduct a network and application penetration test of the production environment at least annually. With Clutch, Inc. tracks critical or high-risk findings through resolution.	Inspected the penetration testing to determine that the company engages a third party to conduct a network and application penetration test of the production environment at least annually. The company tracks critical or high-risk findings through resolution.	No exceptions noted.
CC 2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Security commitments and expectations are communicated to external users via the company's website.	Inspected the company security page or company terms to determine that security commitments and expectations are communicated to external users via the company's website.	No exceptions noted.
	The company publishes its Privacy Policy to both external users and internal personnel. This policy details the company's privacy commitments.	Inspected Company Privacy Policy to determine that it is published to both external users and internal personnel and this policy details the company's privacy commitments.	No exceptions noted.
	The With Clutch, Inc.'s Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected Security Incident Response Policy to determine that it outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	No exceptions noted.
	With Clutch, Inc. has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of non-compliance. In addition, internal personnel acknowledges the Code of Conduct promptly on hire.	Inspected the company's Code of Conduct Policy and list of current employees to determine that the policy is in place outlining ethical expectations, behavior standards, and ramifications of non-compliance, and internal personnel acknowledges the Code of Conduct promptly on hire.	No exceptions noted.
	Senior management and/or BOD meets at least annually to review business objectives, company initiatives, resource needs, and risk management activities.	Inspected the company's list of the board of directors or any equivalent entity function, and meeting minutes to determine that they meet at least annually to review business objectives, company initiatives, resource needs, and risk management activities.	No exceptions noted.
	Internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security, availability, and confidentiality.	Inspected the list of current employees to determine that internal personnel complete annual training programs for information security, to help them understand their obligations and responsibilities related to security, availability, and confidentiality.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of With Clutch, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	Management publishes the Acceptable Use policy to internal personnel. In addition, internal personnel acknowledges these procedures within 60 days of hire.	Inspected the company's Acceptable Use Policy and list of current employees to determine that management publishes the policy to internal personnel, and in addition, internal personnel acknowledges these procedures within 60 days on hire.	No exceptions noted.
	Management publishes the Data Classification Policy to internal personnel. In addition, internal personnel acknowledges these procedures within 60 days of hire.	Inspected the company's Data Classification Policy and list of current employees to determine that management publishes the policy to internal personnel, and in addition, internal personnel acknowledges these procedures within 60 days on hire.	No exceptions noted.
	Management publishes the Information Security Policy to internal personnel. In addition, internal personnel acknowledges these procedures within 60 days of hire.	Inspected the company's Information Security Policy and list of current employees to determine that management publishes the policy to internal personnel, and in addition, internal personnel acknowledges these procedures within 60 days on hire.	No exceptions noted.
	With Clutch, Inc. management is responsible for the design, implementation, and management of the organization’s security policies and procedures. The policies and procedures are periodically reviewed.	Inspected the company's security policies and its version history to determine that management is responsible for the design, implementation, and management of the organization’s security policies and procedures. The policies and procedures are periodically reviewed.	No exceptions noted.
CC 2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Security commitments and expectations are communicated to external users via the company's website.	Inspected the company security page or company terms to determine that security commitments and expectations are communicated to external users via the company's website.	No exceptions noted.
	With Clutch, Inc. publishes or shares its Terms of Service to both internal personnel and external users. These Terms of Service detail the company's confidentiality commitments.	Inspected the company Terms of Service to determine that With Clutch, Inc. publishes or shares its Terms of Service to both internal personnel and external users and these Terms of Service detail the company's confidentiality commitments.	No exceptions noted.
	With Clutch, Inc. communicates critical information to customers and other external parties, as applicable.	Inspected documentation to determine that With Clutch, Inc. communicates critical information to customers and other external parties, as applicable.	No exceptions noted.
	With Clutch, Inc. has a confidential reporting channel available to internal personnel and external users to report security and other identified concerns.	Inspected documentation to determine that With Clutch, Inc. has a confidential reporting channel available to internal personnel and external users to report security and other identified concerns.	No exceptions noted.
	The company publishes its Privacy Policy to both external users and internal personnel. This policy details the	Inspected Company Privacy Policy to determine that it is published to both external users and internal personnel and this policy details the company's privacy commitments.	No exceptions noted.

Trust Services Criteria for the Security Category	***Description of With Clutch, Inc.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
	company's privacy commitments.		
Risk Assessment			
CC 3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Management performs a formal review of the Risk Assessment and Management Policy at least annually. Risk tolerance and strategies are defined in the policy.	Inspected the company's Risk Assessment Policy to determine that management performs a formal review of the policy at least annually. Risk tolerance and strategies are defined in the policy.	No exceptions noted.
	With Clutch, Inc. performs a formal risk assessment, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected company's records to determine that they perform a formal risk assessment, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No exceptions noted.
CC 3.2 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.	With Clutch, Inc. maintains a list of the company's system components and owners.	Inspected documentation to determine that With Clutch, Inc. maintains a list of the company's system components and owners.	No exceptions noted.
	With Clutch, Inc. performs a formal risk assessment, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected company's records to determine that they perform a formal risk assessment, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No exceptions noted.
	With Clutch, Inc. maintains a risk register, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	Inspected company records to determine that they maintain a risk register, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	No exceptions noted.
	With Clutch, Inc.'s Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle. With Clutch, Inc. assess new vendors according to the Vendor Risk Management Policy before engaging with the vendor.	Inspected the company's Vendor Management Policy to determine that it defines a framework for the onboarding and management of the vendor relationship lifecycle. The company assess new vendors according to the Vendor Risk Management Policy before engaging with the vendor.	No exceptions noted.
	The relationship owner collects and reviews the SOC reports (or equivalent) of its subservice organizations on an annual basis.	Inspected the list of vendors to determine that the relationship owner collects and reviews the SOC reports (or equivalent) of its subservice organizations on an annual basis.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of With Clutch, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
CC 3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	With Clutch, Inc. performs a formal risk assessment, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected company's records to determine that they perform a formal risk assessment, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No exceptions noted.
CC 3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Management performs a formal review of the Risk Assessment and Management Policy at least annually. Risk tolerance and strategies are defined in the policy.	Inspected the company's Risk Assessment Policy to determine that management performs a formal review of the policy at least annually. Risk tolerance and strategies are defined in the policy.	No exceptions noted.
	With Clutch, Inc.'s Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle. With Clutch, Inc. assess new vendors according to the Vendor Risk Management Policy before engaging with the vendor.	Inspected the company's Vendor Management Policy to determine that it defines a framework for the onboarding and management of the vendor relationship lifecycle. The company assess new vendors according to the Vendor Risk Management Policy before engaging with the vendor.	No exceptions noted.
Monitoring Activities			
CC 4.1 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.	System owners conduct at least annual user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.	Inspected the company's access security to determine that system owners conduct at least annual user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.	No exceptions noted.
	With Clutch, Inc. has a continuous monitoring solution for internal controls used in the achievement of Company’s service commitments and system requirements.	Inspected the company's infrastructure and version control tool to determine that they have a continuous monitoring solution for internal controls used in the achievement of the Company’s service commitments and system requirements.	No exceptions noted.
	Vulnerability scanning is performed on production infrastructure systems. With Clutch, Inc. remediates identified deficiencies on a timely basis.	Inspected company records to determine that vulnerability scanning is performed on production infrastructure systems. The company remediates identified deficiencies on a timely basis.	No exceptions noted.
	With Clutch, Inc. engages a third party to conduct a network and application penetration test of the production environment at least annually. With Clutch, Inc. tracks critical or high-risk findings through resolution.	Inspected the penetration testing to determine that the company engages a third party to conduct a network and application penetration test of the production environment at least annually. The company tracks critical or high-risk findings through resolution.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of With Clutch, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
CC 4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies on time to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	System owners conduct at least annual user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.	Inspected the company's access security to determine that system owners conduct at least annual user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.	No exceptions noted.
	Senior management and/or BOD meets at least annually to review business objectives, company initiatives, resource needs, and risk management activities.	Inspected the company's list of the board of directors or any equivalent entity function, and meeting minutes to determine that they meet at least annually to review business objectives, company initiatives, resource needs, and risk management activities.	No exceptions noted.
	With Clutch, Inc. has a continuous monitoring solution for internal controls used in the achievement of Company’s service commitments and system requirements.	Inspected the company's infrastructure and version control tool to determine that they have a continuous monitoring solution for internal controls used in the achievement of the Company’s service commitments and system requirements.	No exceptions noted.
	Vulnerability scanning is performed on production infrastructure systems. With Clutch, Inc. remediates identified deficiencies on a timely basis.	Inspected company records to determine that vulnerability scanning is performed on production infrastructure systems. The company remediates identified deficiencies on a timely basis.	No exceptions noted.
	With Clutch, Inc. engages a third party to conduct a network and application penetration test of the production environment at least annually. With Clutch, Inc. tracks critical or high-risk findings through resolution.	Inspected the penetration testing to determine that the company engages a third party to conduct a network and application penetration test of the production environment at least annually. The company tracks critical or high-risk findings through resolution.	No exceptions noted.
Control Activities			
CC 5.1 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.	With Clutch, Inc. maintains a list of the company's system components and owners.	Inspected documentation to determine that With Clutch, Inc. maintains a list of the company's system components and owners.	No exceptions noted.
	With Clutch, Inc. performs a formal risk assessment, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected company's records to determine that they perform a formal risk assessment, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of With Clutch, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	With Clutch, Inc. maintains a risk register, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	Inspected company records to determine that they maintain a risk register, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	No exceptions noted.
CC 5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	With Clutch, Inc.'s Change Management Policy governs the system development life cycle, including documented policies for tracking, testing, and approving changes.	Inspected the Change Management Policy to determine that it governs the system development life cycle, including documented policies for tracking, testing, and approving changes.	No exceptions noted.
	Management publishes the Data Classification Policy to internal personnel. In addition, internal personnel acknowledges these procedures within 60 days of hire.	Inspected the company's Data Classification Policy and list of current employees to determine that management publishes the policy to internal personnel, and in addition, internal personnel acknowledges these procedures within 60 days on hire.	No exceptions noted.
	With Clutch, Inc.'s Policies outline roles and responsibilities for personnel with responsibility for the security, availability, and confidentiality of the system.	Inspected the company policies to determine that they outline roles and responsibilities for personnel with responsibility for the security, availability, and confidentiality of the system.	No exceptions noted.
	With Clutch, Inc.'s Data Classification Policy and Acceptable Use Policy details the security and handling protocols for sensitive data.	Inspected the company's Data Classification Policy and Acceptable Use Policy to determine that they detail the security and handling protocols for sensitive data.	No exceptions noted.
CC 5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	With Clutch, Inc. has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of non-compliance. In addition, internal personnel acknowledges the Code of Conduct promptly on hire.	Inspected the company's Code of Conduct Policy and list of current employees to determine that the policy is in place outlining ethical expectations, behavior standards, and ramifications of non-compliance, and internal personnel acknowledges the Code of Conduct promptly on hire.	No exceptions noted.
	Management publishes the Acceptable Use policy to internal personnel. In addition, internal personnel acknowledges these procedures within 60 days of hire.	Inspected the company's Acceptable Use Policy and list of current employees to determine that management publishes the policy to internal personnel, and in addition, internal personnel acknowledges these procedures within 60 days on hire.	No exceptions noted.
	Management publishes the Data Classification Policy to internal personnel. In addition, internal personnel acknowledges these procedures within 60 days of hire.	Inspected the company's Data Classification Policy and list of current employees to determine that management publishes the policy to internal personnel, and in addition, internal personnel acknowledges these procedures within 60 days on hire.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of With Clutch, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	Management publishes the Information Security Policy to internal personnel. In addition, internal personnel acknowledges these procedures within 60 days of hire.	Inspected the company's Information Security Policy and list of current employees to determine that management publishes the policy to internal personnel, and in addition, internal personnel acknowledges these procedures within 60 days on hire.	No exceptions noted.
	With Clutch, Inc. management is responsible for the design, implementation, and management of the organization’s security policies and procedures. The policies and procedures are periodically reviewed.	Inspected the company's security policies and its version history to determine that management is responsible for the design, implementation, and management of the organization’s security policies and procedures. The policies and procedures are periodically reviewed.	No exceptions noted.
Logical and Physical Access			
CC 6.1 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.	With Clutch, Inc. maintains a list of the company's system components and owners.	Inspected documentation to determine that With Clutch, Inc. maintains a list of the company's system components and owners.	No exceptions noted.
	Users are assigned unique IDs to access sensitive information.	Inspected company records to determine that users are assigned unique IDs to access sensitive information.	No exceptions noted.
	Internal user access to systems and applications with customer data requires a form of two-factor authentication, where available.	Inspected company records to determine if internal user access to systems and applications with customer data requires a form of two-factor authentication, where available.	No exceptions noted.
	With Clutch, Inc. has formal policies for password complexity and length and the use of authentication mechanisms, when available.	Inspected company records to determine that With Clutch, Inc. has formal policies for password complexity and length and the use of authentication mechanisms, when available.	No exceptions noted.
	Production infrastructure is restricted to users with a unique account, SSH key or access key	Inspected documentation to determine that production infrastructure is restricted to users with a unique account, SSH key or access key.	No exceptions noted.
	Administrative access to production servers, databases, and internal administrative tools is restricted based on the principle of least privilege.	Inspected company records to determine that administrative access to production servers, databases, and internal administrative tools is restricted based on the principle of least privilege.	No exceptions noted.
	Users are provisioned access to systems based on principle of least privilege.	Inspected company records to determine that users are provisioned access to systems based on principle of least privilege.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of With Clutch, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	Upon termination or when internal personnel no longer require access, infrastructure and application access is removed, as applicable.	Inspected the company's access security to determine that upon termination or when internal personnel no longer require access, infrastructure and application access is removed, as applicable.	No exceptions noted.
	Service data is encrypted at rest.	Inspected the company's data security to determine that service data is encrypted at rest.	No exceptions noted.
	With Clutch, Inc.'s Encryption and Key Management Policy supports the secure encryption and decryption of app secrets, and governs the use of cryptographic controls.	Inspected the Encryption and Key Management Policy to determine that they support the secure encryption and decryption of app secrets and that they govern the use of cryptographic controls.	No exceptions noted.
CC 6.2 Before 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.	Users are provisioned access to systems based on principle of least privilege.	Inspected company records to determine that users are provisioned access to systems based on principle of least privilege.	No exceptions noted.
	Upon termination or when internal personnel no longer require access, infrastructure and application access is removed, as applicable.	Inspected the company's access security to determine that upon termination or when internal personnel no longer require access, infrastructure and application access is removed, as applicable.	No exceptions noted.
	System owners conduct at least annual user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.	Inspected the company's access security to determine that system owners conduct at least annual user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.	No exceptions noted.
CC 6.3 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.	Administrative access to production servers, databases, and internal administrative tools is restricted based on the principle of least privilege.	Inspected company records to determine that administrative access to production servers, databases, and internal administrative tools is restricted based on the principle of least privilege.	No exceptions noted.
	Users are provisioned access to systems based on principle of least privilege.	Inspected company records to determine that users are provisioned access to systems based on principle of least privilege.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of With Clutch, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	Upon termination or when internal personnel no longer require access, infrastructure and application access is removed, as applicable.	Inspected the company's access security to determine that upon termination or when internal personnel no longer require access, infrastructure and application access is removed, as applicable.	No exceptions noted.
	System owners conduct at least annual user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.	Inspected the company's access security to determine that system owners conduct at least annual user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.	No exceptions noted.
CC 6.4 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.	The entity does not operate any physical hardware such as servers and network devices but rather uses subservice organizations and relies on its controls for physical access.	Not Applicable - Control is implemented and maintained by sub service organizations.	No exceptions noted.
CC 6.5 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.	Media handling and disposal procedures are in place to guide personnel in performing sanitization procedures on all accounts where production data resides so that data and software is unrecoverable before retiring the asset, when managed such asset is directly managed by the company.	Inspected the company's Asset Management Policy and configurations to determine that there is a policy in place to guide personnel in performing sanitization procedures on all accounts where production data resides so that data and software is unrecoverable before retiring the asset, when managed such asset is directly managed by the company.	No exceptions noted.
	Management performs an annual review of the subservice organization’s SOC 2 report/s for issues that may impact the security, availability, or confidentiality of the System. Issues found in the review are evaluated and are documented in the Vendor Risk Assessment.	Inspected the company's Vendor Risk Management Policy to determine that management performs an annual review of the subservice organization’s SOC 2 report/s for issues that may impact the security, availability, or confidentiality of the System. Issues found in the review are evaluated and are documented in the Vendor Risk Assessment.	No exceptions noted.
CC 6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Production infrastructure is restricted to users with a unique account, SSH key or access key	Inspected documentation to determine that production infrastructure is restricted to users with a unique account, SSH key or access key.	No exceptions noted.
	Encryption is used to protect the transmission of data over the internet.	Inspected the company's data security to determine that encryption is used to protect the transmission of data over the internet.	No exceptions noted.
	Configurations ensure available networking ports and protocols are restricted as necessary.	Inspected the company's System Security to determine that configurations ensure available networking ports and protocols are restricted as necessary.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of With Clutch, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	With Clutch, Inc.'s Encryption and Key Management Policy supports the secure encryption and decryption of app secrets, and governs the use of cryptographic controls.	Inspected the Encryption and Key Management Policy to determine that they support the secure encryption and decryption of app secrets and that they govern the use of cryptographic controls.	No exceptions noted.
CC 6.7 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.	Administrative access to production servers, databases, and internal administrative tools is restricted based on the principle of least privilege.	Inspected company records to determine that administrative access to production servers, databases, and internal administrative tools is restricted based on the principle of least privilege.	No exceptions noted.
	Service data is encrypted at rest.	Inspected the company's data security to determine that service data is encrypted at rest.	No exceptions noted.
	Encryption is used to protect the transmission of data over the internet.	Inspected the company's data security to determine that encryption is used to protect the transmission of data over the internet.	No exceptions noted.
	With Clutch, Inc. encrypts hard drives for portable endpoints with full disk encryption.	Inspected company workstations/computers to determine that they encrypt hard drives for portable endpoints with full disk encryption.	No exceptions noted.
CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	With Clutch, Inc.'s Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy and Change Management Plan to determine that Configuration and Asset Management Policy governs configurations for new sensitive systems.	No exceptions noted.
	With Clutch, Inc.'s Change Management Policy governs the system development life cycle, including documented policies for tracking, testing, and approving changes.	Inspected the Change Management Policy to determine that it governs the system development life cycle, including documented policies for tracking, testing, and approving changes.	No exceptions noted.
	Company endpoints are managed via MDM or equivalent.	Inspected company workstations/computers to determine that company endpoints are managed via MDM or equivalent.	No exceptions noted.
System Operations			
CC 7.1 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.	With Clutch, Inc.'s Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy and Change Management Plan to determine that Configuration and Asset Management Policy governs configurations for new sensitive systems.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of With Clutch, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	With Clutch, Inc.'s Vulnerability Management Program outlines the procedures to identify, assess, and remediate identified vulnerabilities.	Inspected the Vulnerability and Patch Management Policy to determine that the policy outlines the procedures to identify, assess, and remediate identified vulnerabilities.	No exceptions noted.
	Vulnerability scanning is performed on production infrastructure systems. With Clutch, Inc. remediates identified deficiencies on a timely basis.	Inspected company records to determine that vulnerability scanning is performed on production infrastructure systems. The company remediates identified deficiencies on a timely basis.	No exceptions noted.
	With Clutch, Inc. engages a third party to conduct a network and application penetration test of the production environment at least annually. With Clutch, Inc. tracks critical or high-risk findings through resolution.	Inspected the penetration testing to determine that the company engages a third party to conduct a network and application penetration test of the production environment at least annually. The company tracks critical or high-risk findings through resolution.	No exceptions noted.
CC 7.2 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.	Management has implemented tools to provide monitoring of network traffic to the production environment.	Inspected the company's system security to determine that management has implemented tools to provide monitoring of network traffic to the production environment.	No exceptions noted.
	With Clutch, Inc. uses logging and monitoring software to collect data from servers, detect potential security threats and unusual system activity and monitor system performance.	Inspected the company's system security to determine that they use logging and monitoring software to collect data from servers, detect potential security threats and unusual system activity, and monitor system performance.	No exceptions noted.
	With Clutch, Inc. uses alerting software to notify impacted teams of potential security and availability events.	Inspected the company's system security to determine that they use alerting software to notify impacted teams of potential security and availability events.	No exceptions noted.
CC 7.3 The entity evaluates security events to determine whether they could or have failed the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company publishes its Privacy Policy to both external users and internal personnel. This policy details the company's privacy commitments.	Inspected Company Privacy Policy to determine that it is published to both external users and internal personnel and this policy details the company's privacy commitments.	No exceptions noted.
	The With Clutch, Inc.'s Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected Security Incident Response Policy to determine that it outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of With Clutch, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	With Clutch, Inc. tracks identified incidents according to the Incident Response Plan.	Inspected Security Incident Response Policy to determine that With Clutch, Inc. tracks identified incidents according to the Incident Response Plan.	No exceptions noted.
CC 7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	With Clutch, Inc. tracks identified incidents according to the Incident Response Plan.	Inspected Security Incident Response Policy to determine that With Clutch, Inc. tracks identified incidents according to the Incident Response Plan.	No exceptions noted.
	With Clutch, Inc. requires a 'lessons learned' document after each incident and shares this document with the Engineering team to make any required changes.	Inspected the Incident Response Policy to determine that With Clutch, Inc. requires a 'lessons learned' document after each incident and shares this document with the Engineering team to make any required changes.	No exceptions noted.
CC 7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	With Clutch, Inc. tracks identified incidents according to the Incident Response Plan.	Inspected Security Incident Response Policy to determine that With Clutch, Inc. tracks identified incidents according to the Incident Response Plan.	No exceptions noted.
	With Clutch, Inc. requires a 'lessons learned' document after each incident and shares this document with the Engineering team to make any required changes.	Inspected the Incident Response Policy to determine that With Clutch, Inc. requires a 'lessons learned' document after each incident and shares this document with the Engineering team to make any required changes.	No exceptions noted.
Change Management			
CC 8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	System changes are tested before being deployed into production.	Inspected the Change Management Plan to determine that system changes are tested before being deployed into production.	No exceptions noted.
	Code merge requests are independently peer-reviewed before integrating the code change into the master branch and system users who make changes are unable to deploy their changes without independent approval.	Inspected the Change Management Plan to determine that code merge requests are independently peer-reviewed before integrating the code change into the master branch and system users who make changes are unable to deploy their changes without independent approval.	No exceptions noted.
	The production and staging environments are segregated.	Inspected the Change Management Plan to determine that the production and staging environments are segregated.	No exceptions noted.
	Production data is not used in the development and testing environments.	Inspected the Change Management Plan to determine that production data is not used in the development and testing environments.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of With Clutch, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	With Clutch, Inc.'s Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy and Change Management Plan to determine that Configuration and Asset Management Policy governs configurations for new sensitive systems.	No exceptions noted.
	With Clutch, Inc.'s Change Management Policy governs the system development life cycle, including documented policies for tracking, testing, and approving changes.	Inspected the Change Management Policy to determine that it governs the system development life cycle, including documented policies for tracking, testing, and approving changes.	No exceptions noted.
	Descriptions of the company's services are available to both internal personnel and external users.	Inspected the Company Product Page for external users and Network Diagram for internal users to determine that descriptions of the company's services are available to both internal personnel and external users.	No exceptions noted.
Risk Mitigation			
CC 9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The With Clutch, Inc.'s Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected Security Incident Response Policy to determine that it outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	No exceptions noted.
	With Clutch, Inc. performs a formal risk assessment, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected company's records to determine that they perform a formal risk assessment, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No exceptions noted.
	With Clutch, Inc. maintains a risk register, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	Inspected company records to determine that they maintain a risk register, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	No exceptions noted.
	With Clutch, Inc. maintains business continuity and disaster recovery plan. With Clutch, Inc. periodically tests its Business Continuity and Disaster Recovery Plan. When necessary, Management makes changes to the Business Continuity and Disaster Recovery Plan based on the test results.	Inspected the Business Continuity and Disaster Recovery Policy to determine that management periodically tests its Business Continuity and Disaster Recovery Plan and makes changes based on the test results, when necessary.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of With Clutch, Inc.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
CC 9.2 The entity assesses and manages risks associated with vendors and business partners.	With Clutch, Inc.'s Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle. With Clutch, Inc. assesses new vendors according to the Vendor Risk Management Policy before engaging with the vendor.	Inspected the company's Vendor Management Policy to determine that it defines a framework for the onboarding and management of the vendor relationship lifecycle. The company assesses new vendors according to the Vendor Risk Management Policy before engaging with the vendor.	No exceptions noted.
	The relationship owner collects and reviews the SOC reports (or equivalent) of its subservice organizations on an annual basis.	Inspected the list of vendors to determine that the relationship owner collects and reviews the SOC reports (or equivalent) of its subservice organizations on an annual basis.	No exceptions noted.