Pollen, Inc.
Report on Controls at a Service Organization Relevant to Security, Availability, and Processing Integrity

SOC 3℠ Report

For the Period July 1, 2019 through June 30, 2020

SOC 3 is a registered service mark of the American Institute of Certified Public Accountants (AICPA)
Independent Service Auditor’s Report

To the Management of Pollen, Inc. (C2FO):

Scope

We have examined C2FO's accompanying assertion titled "Assertion of C2FO Management" (assertion) that the controls within C2FO's C2FO System (system) were effective throughout the period July 1, 2019 to June 30, 2020, to provide reasonable assurance that C2FO's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and processing integrity (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Service Organization's Responsibilities

C2FO 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 C2FO's service commitments and system requirements were achieved. C2FO has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, C2FO is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management’s assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve C2FO’s service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve C2FO's service commitments and system requirements based on the applicable trust services criteria

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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management’s assertion that the controls within C2FO’s C2FO system were effective throughout the period July 1, 2019 to June 30, 2020, to provide reasonable assurance that C2FO’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

BARR Advisory, P.A.

Fairway, KS
July 14, 2020
Assertion of C2FO Management

We are responsible for designing, implementing, operating, and maintaining effective controls within C2FO's C2FO system (system) throughout the period July 1, 2019 to June 30, 2020, to provide reasonable assurance that C2FO’s service commitments and system requirements relevant to security, availability, and processing integrity were achieved. Our attached system description of the C2FO system identified the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2019 to June 30, 2020, to provide reasonable assurance that C2FO’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and processing integrity (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). C2FO's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the attached system description.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period July 1, 2019 to June 30, 2020, to provide reasonable assurance that C2FO's service commitments and system requirements were achieved based on the applicable trust services criteria.

Pollen, Inc.
August 14, 2020
Overview of Operations

Company Background

Pollen, Inc. (C2FO) is a financial technology company and the creator of the first market for working capital. C2FO provides a transparent marketplace for companies to deploy and secure working capital, bringing buyers and their suppliers together in a live marketplace without intermediaries to find a real-time rate for cash flow.

The C2FO utility based pricing model allows cash to flow freely between companies at a rate that works for everyone. Using the market, suppliers can request early payment from buyers on approved invoices. If early payment is awarded, the funds are facilitated directly through the buyer to the supplier via their current payment channels.

C2FO helps buyers increase gross margin and EBITDA, generate higher returns on cash, improve the financial health of their supply chain, and complement existing early payment programs. In addition, C2FO helps suppliers improve cash flow, access early payment of invoices on demand, and eliminate paperwork and contracts through an online platform.

Products and Services

The Collaborative Cash Flow Optimization (C2FO) system operates as a Software as a Service (SaaS) cloud computing model. The main platform allows buyers and suppliers to collaborate in a transparent fashion to negotiate discounts on invoices in return for early payment.

A “buyer” in the C2FO platform is a business looking to generate income from accounts payable invoices. These buyers are most likely in a position where they have a substantial amount of cash on their balance sheet, and are looking to generate larger returns, as compared to what they are offered with other low-risk liquid investment options.

A “supplier” in the C2FO platform is a business willing to offer discounts on accounts receivable invoices in exchange for nearly immediate payment. In most instances, these are small to medium-size businesses that need more cash flow to make payroll, rent, or to pay their own suppliers. These suppliers know what their cost of borrowing is and look to find financial tools that provide them with cash leverage at lower rates. Many suppliers only need stronger cash flow during specific times of the year, while others require better cash flow throughout all times of the year.

Buyers configure an expected rate of return in the C2FO market, while the supplier sets the rate they are willing to discount against an invoice. These rates are used in algorithms to determine “matches” between buyers and suppliers, and in effect, connect businesses with one another that have compatibility with rate of return and discount. When matches are made, the supplier is notified and expects payment within the defined payment cycle of the buyer, in most instances, within two days. The same day, the C2FO market provides the buyer a flat file that denotes the rate that matched with each supplier invoice. The flat file is used by the buyer’s accounts payable team to remit payment to suppliers according to the contracted payment schedule and rate.

Suppliers in the C2FO platform may change their rates in the system as often as needed and only make offers when desired. Similarly, buyers in the C2FO platform may change their rates as often as desired, provide only approved-to-pay invoices into the market, and set a cash pool to denote the amount of approved invoices they are willing to pay early. With all of these functions, the C2FO market is designed to provide both suppliers and buyers with the most protection as possible, along with flexibility to participate at their chosen comfort level.
Available for both buyers and suppliers

Global capabilities:

- Multilingual help available, including English, Spanish, German, Dutch, French, Italian, Mandarin, Cantonese, Japanese, Thai, Russian, Hindi, Bengali, and Turkish;
- Multiple currencies supported; and,
- List target returns and set bids by currency.

Reliable technology:

- High-level security standards; and,
- SaaS cloud-based system.

For buyers specifically

Minimal effort:

- ERP friendly solution;
- Simple integration with homegrown systems as well as established ERPs, such as SAP, Oracle, and Lawson;
- Low resource expenditure for buyer implementations (average of 241 technology hours spent);
- Quick implementation; and,
- End-to-end process for a buyer’s market launch averaging eight to 12 weeks, with a technology initiative averaging three to four weeks.

For suppliers specifically

Simple connection:

- No software download required, nor integration with existing tools; and,
- View and interact with the market from a supplier web portal.

Principal Service Commitments and System Requirements

C2FO designs processes and procedures related to the C2FO System to meet certain objectives. Those objectives are based on the service commitments that C2FO makes to user entities, the laws and regulations that govern C2FO System services, and the financial, operational, and compliance requirements that C2FO has established for the services.

Commitments to user entities are documented and communicated in Master Service Agreements (MSAs) 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:

- Access provisioned based on least privilege access principles;
- The use of identity access management software and controls for usernames, passwords, access provisioning and de-provisioning, and role-based access;
- Procedures for managing security incidents and breaches, including notification procedures;
- Regular vulnerability scanning and penetration tests over the C2FO application and
supporting infrastructure components; and,

- Use of boundary protection systems, including firewalls, and intrusion detection systems.

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

- Regular maintenance to be performed outside regular business hours and notice of any emergency maintenance performed outside of documented maintenance windows;
- Real-time information and updates on the status of the C2FO application, including uptime reporting via status.c2fo.com; and,
- Responses to customer-reported issues within 24 business hours for both buyers and suppliers.

Processing integrity commitments are generally standardized and include, but are not limited to, the following:

- Data quality and monitoring procedures or mechanisms to ensure the integrity of files sent to C2FO, processed in the marketplace, and sent back to buyer organizations from C2FO;
- Standard real-time reporting over marketplace data and metrics; and,
- Standard monthly reporting over marketplace data and metrics.

Such requirements are communicated in C2FO’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 C2FO System.

Scope of the Examination

While much of this examination may apply to both “buyers” and “suppliers,” the primary scope of this system examination is focused on the “buyer’s” perspective.

Components of the System

The C2FO System is designed, implemented, and operated to achieve its specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which include the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure and Software

The C2FO applications are Linux-based cloud applications developed and maintained by C2FO’s in-house software engineering team. The internal computing platforms and global infrastructure supporting the C2FO applications are provided by Amazon Web Services (AWS) and Google Cloud Platform (GCP).

The primary applications, systems, infrastructure, and tools are summarized in the tables below.
<table>
<thead>
<tr>
<th>Production System</th>
<th>Business Function Description</th>
<th>Operating System / Database Platform</th>
<th>Physical Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>C2FO Main Webapp</td>
<td>Primary website used by C2FO suppliers and buyers to create and manage accounts, modify contact information, and view information on their marketplaces.</td>
<td>Linux / PostgreSQL</td>
<td>AWS US-West-2 (Oregon) / GCP US-West-1 (Oregon) and GCP Europe-West-3 (Frankfurt)</td>
</tr>
<tr>
<td>C2FO Administration Webapp</td>
<td>Similar to the main web application, but with privileged access restricted to C2FO personnel. It is also used to monitor and control data, and provide production support for buyers and suppliers.</td>
<td>Linux / PostgreSQL</td>
<td>AWS US-West-2 (Oregon) / GCP US-West-1 (Oregon) and GCP Europe-West-3 (Frankfurt)</td>
</tr>
<tr>
<td>C2FO Enterprise Pipeline</td>
<td>Used to transmit files and data between C2FO, buyers, and suppliers.</td>
<td>Linux / PostgreSQL</td>
<td>AWS US-West-2 (Oregon) / GCP US-West-1 (Oregon) and GCP Europe-West-3 (Frankfurt)</td>
</tr>
<tr>
<td>C2FO Asynchronous Jobs</td>
<td>These services perform the calculations that keep the C2FO marketplace running.</td>
<td>Linux / PostgreSQL and RabbitMQ</td>
<td>AWS US-West-2 (Oregon) / GCP US-West-1 (Oregon) and GCP Europe-West-3 (Frankfurt)</td>
</tr>
<tr>
<td>GitHub</td>
<td>Source code repository and version control system.</td>
<td>GitHub Proprietary</td>
<td>GitHub Cloud</td>
</tr>
<tr>
<td>Jenkins</td>
<td>An open-source automation server used to automate the software deployment process, with continuous integration and facilitating technical aspects of continuous delivery.</td>
<td>Jenkins Proprietary</td>
<td>Jenkins Cloud</td>
</tr>
<tr>
<td>Frenzy</td>
<td>Used to manage C2FO's server infrastructure and software deployments.</td>
<td>C2FO Proprietary</td>
<td>AWS US West-2 (Oregon)</td>
</tr>
<tr>
<td>Amazon EC2</td>
<td>A web service that provides resizable compute capacity in the cloud.</td>
<td>Amazon Proprietary</td>
<td>AWS US West</td>
</tr>
</tbody>
</table>
### Primary Infrastructure

<table>
<thead>
<tr>
<th>Production System</th>
<th>Business Function Description</th>
<th>Operating System / Database Platform</th>
<th>Physical Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Compute Engine</td>
<td>Delivers virtual machines running in Google's innovative data centers and worldwide fiber network. Compute Engine's tooling and workflow support enable scaling from single instances to global, load-balanced cloud computing.</td>
<td>Google Proprietary</td>
<td>GCP US West</td>
</tr>
<tr>
<td>Google Kubernetes Engine (GKE)</td>
<td>A managed, production-ready environment for deploying containerized applications, including services for developer productivity, resource efficiency, automated operations, and open-source flexibility.</td>
<td>Google Proprietary</td>
<td>GCP US West</td>
</tr>
<tr>
<td>Amazon Elastic Kubernetes Service (EKS)</td>
<td>Amazon service that makes it easy to deploy, manage, and scale containerized applications using Kubernetes on AWS.</td>
<td>Amazon Proprietary</td>
<td>AWS US West</td>
</tr>
<tr>
<td>Windows Active Directory</td>
<td>Directory service used to authenticate users to C2FO systems.</td>
<td>Windows Server 2012 R2</td>
<td>C2FO Headquarters</td>
</tr>
<tr>
<td>GlobalProtect VPN</td>
<td>Virtual private networking (VPN) software used to restrict access to infrastructure systems.</td>
<td>Palo Alto Networks Proprietary</td>
<td>C2FO Headquarters</td>
</tr>
<tr>
<td>G Suite</td>
<td>Service used for internal communication and access the GCP environment that leverages Windows Active Directory for authentication.</td>
<td>Google Proprietary</td>
<td>GCP US West</td>
</tr>
</tbody>
</table>

### Supporting Software and Tools

<table>
<thead>
<tr>
<th>Production System</th>
<th>Business Function Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JIRA</td>
<td>A customizable tool for agile software development that C2FO uses to log and track progress for bugs, tasks, features, and projects.</td>
</tr>
<tr>
<td>Datadog</td>
<td>A cloud-hosted, agent-based monitoring and alerting tool with approximately 130 integrations for third-party technologies including RabbitMQ, Node.js, and Go. C2FO uses Datadog for custom alerting across most services. C2FO uses Datadog's integration with OpsGenie to alert the on-call engineer or admin in case of an emergency.</td>
</tr>
<tr>
<td>Supporting Software and Tools</td>
<td></td>
</tr>
<tr>
<td>------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Production System</strong></td>
<td><strong>Business Function Description</strong></td>
</tr>
<tr>
<td>Slack</td>
<td>An internal communication and notification system with integrations for multiple third-party products. C2FO uses it to asynchronously contact individuals or targeted groups as needed, without using their SMS or phone services. Slack is accessed through AD credentials, and requires two-factor authentication through SMS or a virtual token such as Google Authenticator. Communications are encrypted and shared files are automatically deleted after 90 days.</td>
</tr>
<tr>
<td>OpsGenie</td>
<td>An alerting and on-call management solution for devops teams. OpsGenie provides the tools needed to design actionable alerts, manage on-call schedules and escalations, and ensure that the right people are notified at the right time, using multiple notification methods. C2FO uses OpsGenie to manage on-call rotations for all of engineering, market operations, and other teams.</td>
</tr>
<tr>
<td>Cavin Pulsar</td>
<td>A security scanning tool created by Cavin which compares infrastructure, operating system, and container settings against common security frameworks, including CIS Benchmarks, SOC 2, and GDPR. This allows C2FO to generate security health reports against those frameworks on demand. Cavin Pulsar also supports a feature-rich API, which helps serve as a baseline for many automated security controls.</td>
</tr>
<tr>
<td>Nessus</td>
<td>A security scanning tool created by Tenable Network Security which uses a variety of security plugins to detect vulnerabilities in network configurations, hosts, and web applications. These plugins are automatically updated with the latest vulnerability definitions.</td>
</tr>
</tbody>
</table>
C2FO’s computing platforms, network technologies, and global infrastructure are provided by third party Infrastructure as a Service (IaaS) cloud service providers. Currently, C2FO operates in a multi-IaaS architecture, which includes instances hosted both by Amazon Web Services (AWS) and Google Cloud Platform (GCP).

**Overall Technical Diagram**

The C2FO application infrastructure includes five primary components: Web Applications, Enterprise Data Pipeline, Market Mechanics, User Authentication Service, and API Gateway.

1. **C2FO Web Applications:**
   a. **Main Webapp:** This is the main website C2FO customers interact with on a regular basis. Customers create and manage their accounts, modify their contact information, and view information on their marketplaces. Account access is password protected.

   - AWS Route53 forwards traffic from app.c2fo.com to the application cluster.

©2020 Pollen, Inc. | All rights reserved | 10
● The cluster sits behind load balancers, which distribute website traffic across site servers.

● User interactions with the web frontend trigger representational state transfer (REST)ful calls to the supporting infrastructure servers.

● These servers perform business logic interactions with the C2FO database, where data access and manipulation is required.

a. **Admin Webapp:** This portion is structured in the same way as the web portal, but with higher-privileged access for C2FO to monitor and control data, and provide production support for customers. Access to the application is password-controlled through C2FO’s internal Active Directory network domain. This service also requires two-factor authentication through a virtual token, such as Google Authenticator, or through a one-time, expiring code sent over SMS to a registered phone number.

2. **Enterprise Pipeline:** This set of services moves data between the C2FO application and buyers as follows:

a. Raw data such as invoices, organizations, divisions, and user information from buyers is processed and saved to the C2FO database to support the platform.

b. Buyers upload their data as CSV files through secure file transfer protocol (SFTP) to ftp.c2fo.com. Each buyer has a security profile unique to their own directory. If requested, C2FO schedules jobs to pull buyer data from their servers to perform the SFTP copy for the buyer. If a buyer prefers, they can upload their files to AWS Simple Storage Solution (S3) instead of using SFTP. Additional S3 secure file transfer details are noted below within the “Technologies in Place” section.

c. Data is copied to S3 where it is encrypted at rest. If the buyer previously elected to upload to S3, it is copied from the S3 bucket to one that can only be accessed by C2FO users and services.

d. Timed service checks for buyer files. To ensure consistent timing of the file load window, during which buyers are able to upload files, C2FO leverages GCP and AWS default timed service checks to synchronize time across EC2 and GCE instances. Found files are analyzed for data integrity including data completeness, expected timing, and expected number of lines. If the files are PGP-encrypted, they are decrypted and rewritten to S3 at this point. Once all of these checks are passed, the file is moved to a different directory on S3 to avoid being reprocessed, and a message is published to RabbitMQ so other services know the file is ready for the process in step “e” below.

e. The content of the files is compiled and stored in a format ready for ingestion into C2FO’s database. Each information type has a specific format and file naming convention. Columns are mapped from the buyers’ custom CSV formats to the C2FO formats. If a customer chooses to upload information of the same type in separate files (e.g., organized by clients), the data are combined into a single file at this point. Once the data translations are complete, the new file is copied to S3 and a message is published to RabbitMQ to start the next step in the process.

f. The formatted CSV files are now analyzed and the data is extracted and saved to the C2FO database. During this process, a number of important data operations are
performed including updates, associations, and deletions.

If at any point an error occurs during this process, the problematic files being uploaded are moved to a temporary invalid directory so that the issue can be addressed and the files reprocessed, if needed. Key information regarding the errors are written to an error journal. This error information is later aggregated and stored to the C2FO database for review by C2FO Admin webapp users.

The second function of Enterprise Pipeline is to go through a similar process to export C2FO marketplace data to the buyers as follows:

a. An award file is generated and written to S3 following a successful market clear. This CSV file has information describing the invoices and companies that were involved in the market clear for that day. When this step is complete, a message is published to RabbitMQ to indicate the file is ready for the next step of processing.

b. Similar to step “e” from above, buyers often store their awarded information in custom formats. At this point, awarded information is processed and mapped from C2FO to the buyer's CSV formats. If the buyer requires PGP encryption, it is done at this time. When the new file is ready, it is saved to S3.

c. A timed job monitors the award file directories from step two for any new files. When one is found, it is copied via SFTP to the buyer’s directory mentioned in step one of the data import process detailed above.

3. **Market Mechanics Services:** These services perform the important calculations that keep the C2FO marketplace running. These are best thought of in four parts:

a. Calculator: This service is the heart of all market mechanics.
   - When a customer changes certain settings, such as desired APR, those changes are saved to a secure caching solution using Redis, which is hosted on AWS Elasticache in AWS and on hosted Docker images in GCP.
   - The service regularly runs over the cached changes and uses them to readjust the market or markets involved.

b. Adjustments: This service applies invoice adjustments based on input received from the buyer through Enterprise Pipeline.

c. Market clear: This service is run every working day at the close of market. It determines which invoices cleared the market for suppliers and starts the process of gathering market statistics and generating award files.

d. Statistics: This service gathers system statistics and compiles them in a way that allows the C2FO data team to better analyze, understand, and improve the product.

4. **User Authentication Service:** This service allows the C2FO webapps to authenticate a user across clouds regardless of the origin of their login session. For example, a user who registered in the EU may log in from the United States. That user's credentials are still stored in the EU, so the User Authentication services would direct any login attempts to the proper data center without having to duplicate a user's credentials across data centers or regions. This is particularly important to satisfy buyers’ Infrastructure as a Service (IaaS) preferences and certain data regulations, such as the European Union’s General Data Protection Regulation (GDPR). These requirements are satisfied in the following manner:
a. A user's email and password are stored in the data center, both region and IaaS provider, in which they were initially created. User creation occurs when a user file is uploaded via eSLAP, in which case the user is stored in the data store of the uploaded eSLAP file. Information for supplier users who self-register is directed to and stored in the nearest IaaS and region by the API Gateway.

b. To avoid distributing a user's data across data centers, and to avoid duplicating users, login email addresses are initially hashed and sent to all user data centers. Based on that hashed email, a data center will identify itself as having that user's information. From that point forth, the API Gateway directs all of the user's REST requests to that data center.

5. **API Gateway**: The Gateway services receive external API calls and route the requests to the proper cloud. As is the case with the User Authentication Service, this feature exists to help satisfy IaaS and data storage requirements from buyers as well as data regulations. This service operates as follows:
   a. Service registration through Consul;
   b. Data center location via user auth; and,
   c. Routing REST calls using the JSON Web Token (JWT) in the request header.

**Software Deployment and Monitoring**

C2FO utilizes an in-house created tool, Frenzy, for deployment of code into AWS managed Elastic Kubernetes Service and GCP managed Google Kubernetes Engine. Instances are deployed using AWS CloudFormation in the US-West-2 region to manage server infrastructure and software deployments and through a combination of Ansible and manual procedures in GCP.

Frenzy uses Git tags to determine the correct branch from which to build an image. It also caches images to improve build times for more commonly built images and then pushes the images to the appropriate registries (e.g., quay.io, DockerHub in AWS, Google Container Registry (gcr.io), etc.). Additionally, Frenzy manages the Helm deployments for Kubernetes in both AWS and GCP. Frenzy creates a new Helm session, updates dependencies for a chart, and then updates or installs a chart if it is new to the cluster.

Frenzy accounts are managed with Windows Active Directory.

**Additional Technologies in Place**

- **Cloud Identity Access Management (IAM)**: Enables the ability to securely control access to cloud services and resources for users. C2FO security administrators create security roles to ensure that access is strictly managed. Roles are associated with users through security groups. Both AWS and GCP have services called IAM.

- **Cloud Hosted Virtual Machines**: C2FO's cloud hosting service includes virtual machine tooling and workflow support to allow scaling from single instances to global, load-balanced cloud computing. C2FO uses these instances to host Linux servers, which provide application logic for all deployment environments. Access to virtual machines is controlled using IAM security roles.

- **Cloud Storage**: Provides developers and IT teams with secure, durable, and highly scalable object storage. This is an important part of the C2FO infrastructure and is used in many processes. Enterprise pipeline uses the technology as a secure staging ground while customer data is decrypted, translated, and saved to the C2FO databases. Cloud storage is
also an important component in uploading data to C2FO's data warehouse solution. It is used to store audit logs for a variety of log monitoring and alerting tools (see below for more on logging technologies). Data in cloud storage files is encrypted at rest with AES128 or better. Access to files is also restricted by security administrators based on IAM roles and bucket-specific security policies. Another important feature is that cloud storage allows nearline and coldline storage for infrequent data access and archiving, respectively. C2FO uses the coldline resource to archive data from the client-facing SFTP server in accordance with the Data Retention Policy. These services are Simple Storage Solution (S3) and Google Cloud Storage (GCS) in AWS and GCP, respectively. In AWS, coldline storage is done with a separate service called Glacier.

- **Key Management Service**: A managed service in AWS and GCP that makes it easy for developers to create and control the encryption keys used to encrypt data. Seamless integration between KMS and cloud storage is an important part of ensuring the security of data at rest.

- **Cloud Load Balancers**: Automatically distributes C2FO traffic across multiple virtual machines. Load balancers provided are AWS Elastic Load Balancers (ELBs) and GCP Load Balancing Service.

- **AWS Simple Storage Service (S3)**: Provides an interface used to store and retrieve business unit data. S3 APIs provide bucket and object level access and version control. S3 is controlled through the AWS IAM interface.

- **Relational Database Service (RDS)**: Allows a user to set up, operate, and scale a relational database in the cloud while managing database administration tasks. C2FO uses RDS to host multiple PostgreSQL instances across different environments and regions. C2FO also uses RDS hosted MySQL instances for tracking deployments that were made using Frenzy.

- **Virtual Private Cloud (VPC)**: Allows C2FO to provision a logically isolated section of the AWS and GCP cloud, where it can launch resources in a virtual network. All C2FO services exist under a single VPC. Subnets within these VPCs are managed using CloudFormation or Terraform. Access to make manual changes to subnets is strictly limited by security administrators.

- **AWS CloudFormation**: Gives developers and system administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. With CloudFormation, a user can describe these series of resources through a JSON-formatted template. In C2FO, these templates are created by developers and uploaded to AWS using Frenzy. These templates are approved through the code management process. The CloudFormation web interface can be accessed by a limited group of users via the AWS IAM console.

- **Terraform**: A tool for building, changing, and versioning infrastructure safely and efficiently. Terraform allows for idempotent multi-cloud infrastructure management. C2FO uses Terraform for new additions and changes to cloud infrastructure in both AWS and GCP.

- **AWS CloudTrail**: A web service that records and logs AWS API calls. The recorded information includes the API caller, time, source IP address request parameters, and response elements. These logs are forwarded to Datadog to allow for metrics, dashboards, alerting, and other capabilities.

- **AWS CloudWatch**: A monitoring and notification service that supports all AWS resources
and applications. C2FO uses this service for alerts, such as high CPU utilization and drop of database connections.

- **Redis**: An open-source, in-memory data store that C2FO uses as a caching solution in some services.

- **AWS ElastiCache**: A web service that makes it easy to deploy, operate, and scale an in-memory cache. C2FO uses Redis, a popular open-source key-value store with master/slave replication as its caching engine. ElastiCache automatically detects and replaces failed nodes. The insight provided through CloudWatch and the AWS Management Console makes this tool particularly useful for managing C2FO’s architecture.

- **AWS Route53**: A highly available and scalable cloud Domain Name System (DNS) web service. C2FO has many domains registered for its variety of international sites.

- **Google Cloud Deployment Manager**: Google Cloud Deployment Manager allows specification of all the resources needed for an application in a declarative format using yaml. C2FO uses Deployment Manager to manage database instances for various deployment environments.

- **GCP Operations**: GCP Operations logging service captures GCP audit logs of GCP API calls, capturing cloud infrastructure reads and writes and data access. C2FO uses Operations to forward application and audit logs to Datadog to allow for metrics, dashboards, alerting, and other capabilities.

- **Ansible**: Ansible is open-source software that allows developers to standardize deployments and configurations. C2FO uses Ansible for some cloud infrastructure provisioning and maintenance tasks in GCP.

- **RabbitMQ**: A popular messaging broker and key part of C2FO's service-based architecture that allows applications to communicate asynchronously. Messages, typically in JSON format, are published from one application and received by another for processing. An advantage to this approach is that it allows C2FO multiple points of scalability based on need. RabbitMQ guarantees that no two applications will process the same message at once, so developers can deploy as many applications that monitor for the same type of data as is needed. It is also used to publish errors from applications for real time alerting and handling. RabbitMQ provides a web interface for developers to review the status of the different queues and channels. There are also several integration tools that can alert of suspicious activity, such as a queue that has grown too large. Access to this web interface is password protected.

- **Docker**: A software tool that allows C2FO to package an application with all of its dependencies into a standardized unit for software development. Containers wrap up a piece of software in a complete filesystem that contains everything required to run the software, ensuring that the software will always run the same regardless of the environment. The Docker containers for the C2FO application are deployed through Frenzy using Helm charts to Elastic Kubernetes Service (EKS) in AWS and Google Kubernetes Engine (GKS) in GCP.

- **Consul**: Consul makes it simple for services to register themselves and to discover other services via a DNS or HTTP interface and register external services, such as SaaS providers. C2FO uses this tool to support the gateway portion of the product infrastructure, which is a key part of running in a multi-regional, multi-cloud architecture.
• **Node.js and NPM**: A JavaScript runtime built on Chrome's V8 JavaScript engine. Node.js uses an event-driven, non-blocking I/O model that makes it lightweight and efficient. Node.js' package ecosystem, NPM, is the largest ecosystem of open-source libraries in the world.

• **The Go Programming Language**: An open-source programming language that makes it easy to build simple, reliable, and efficient software.

• **Scala**: A programming language that runs on the JVM. Scala is built for scalable applications and serves as the main programming language for the API Gateway and a number of services running as part of Market Mechanics.

**Achieving Scalability**

Scalability is of critical importance to C2FO. C2FO follows service-oriented architecture concepts that provide decoupled, modular services. Operating within a cloud infrastructure allows C2FO to scale these services on the fly, both horizontally and vertically.

**Achieving High Performance**

For the web service, C2FO has a strict requirement of response times of less than 2000ms for web page rendering. This is achieved by keeping the code algorithmically efficient, reducing the number of layers, and using caching where applicable. At the database layer, high performance is achieved through a data model designed with appropriate indexes to facilitate access patterns. Additionally, regularly scheduled performance tests are analyzed and important architectural decisions are made to ensure that all applications perform at acceptable levels.

**Achieving High Availability**

High availability is one of the most important architectural considerations at C2FO. In order to help ensure high availability of C2FO services, C2FO ensures all services are deployed and live across multiple availability zones (multi-AZ) within the primary IaaS regions. For compute instances that C2FO instantiates and manages, C2FO's deployment system manages the multi-AZ deployment. AWS and GCP provide services that support multi-AZ automatically, such as load balancing which is used where routing is needed to manage access to the multi-AZ assets.

**Achieving High Security**

The C2FO website is only accessible over TLS 1.2 or higher. C2FO internal users are authenticated via Windows Active Directory to access their personal information within their profiles. C2FO clients access publicly facing servers either with SFTP or HTTPS. Besides the functional aspect of the site, role-based security is used for C2FO site administration, customer care, and other administration. All customer data is encrypted both in transit and at rest. In addition, C2FO uses both Nessus and Cavirin Pulsar to scan infrastructure and service hosts for known security vulnerabilities and bad practices.

**Monitoring Performance, Scalability, and Availability**

Performance monitoring in C2FO is done using Datadog and Pingdom. Besides that monitoring, for redundancy purposes, C2FO uses Pingdom.io for monitoring uptime to the C2FO websites and APIs. All webapp security access events are recorded and logged to Papertrail.

**People**

C2FO currently has approximately 450 employees globally. C2FO is headquartered in Leawood, Kansas, and has other offices at the following locations: Seattle, London, Frankfurt, Mumbai, Noida,
Beijing, Shenzhen, Hong Kong, and Singapore.

**Procedures**

Formal IT policies and procedures exist that describe incident response, network security, encryption, and system security standards. All teams are expected to adhere to C2FO policies and procedures that define how services should be delivered. These are located on the company's shared drive and can be accessed by any C2FO team member.

The policies, standards, and procedures used to safeguard C2FO systems and data include:

- Information Security Policy
- Acceptable Use Standard
- Data Protection Standard
- Personnel Security Standard
- Disciplinary Procedure
- Individual Rights Request Procedures
- Onboarding, Transfer, and Offboard Procedures
- Engineering Account Access Management Procedure
- Access Control Standard
- Application Development Security Standard
- Technical Security Standard
- Physical Security Standard
- Risk Management Procedure
- Application Change Management Procedure
- Vendor Management Procedure
- Security Incident Management Procedure
- Vulnerability Management Procedure
- Security Incident Contact List
- Internal Audit Procedures
- Data Destruction Procedure
- Information Classification and Labeling Procedures
- Information Security Incident Management Standard
- Information Security Program Standard

**Data**

C2FO platform processes and stores many data elements from its clients to include information about:

- Invoices
- Users
- Organizations
- Divisions

Users are required to provide an email address and password to provision their account and operate the web or mobile front end. All data is stored in Amazon RDS, S3 buckets, Google Cloud Storage, or Google Compute Engine Postgres instances, depending on the infrastructure provider, and is encrypted at rest.
Complementary User Entity Controls

C2FO controls were designed with the assumption that certain internal controls would be in place at client organizations. The application of such internal controls by client organizations is necessary to achieve certain criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for the processing of transactions for C2FO clients related to the information processed.

For clients to rely on the information processed through C2FO applications, each client is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures are controls to be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by client organizations.

- User entities are responsible for protecting established user IDs and passwords within their organizations;
- User entities are responsible for sending data to C2FO via a secure connection and/or the data should be encrypted;
- User entities are responsible for notifying C2FO if they detect or suspect a security incident related to the C2FO System;
- User entities are responsible for reviewing email and other forms of communication from C2FO related to changes that may affect the C2FO customers and users, and their security, availability, and processing integrity;
- User entities are responsible for establishing, monitoring, and maintaining controls over processing integrity for system-generated outputs and reports from the C2FO System;
- User entities are responsible for establishing, monitoring, and maintaining controls over adjustment files communicated to C2FO as well as the timeliness of adjustment files communicated to C2FO;
- User entities are responsible for testing C2FO System integrations to buyer systems in accordance with agreed upon project implementation plans;
- User entities are responsible for testing independently verifying code changes to ensure the accuracy and propriety of maintenance changes;
- User entities are responsible for using a web browser that supports strong encryption methods and protocols when accessing C2FO systems;
- User entities are responsible for keeping their own computer networks and equipment free of spyware, viruses, sniffers, and other malware; and,
- User entities are responsible for ensuring proper controls are in place when they elect to opt out of system features including, but not limited to, the following:
  - PGP encryption;
  - Control files for daily award files;
  - Receiving empty award files; and/or,
  - Automatically receive award files.
Complementary Subservice Organization Controls

C2FO uses subservice organizations for data center, infrastructure, software, and managed hosting services in support of its production applications. C2FO periodically reviews the quality of the outsourced operations by various methods including:

- Review of subservice organizations' SOC 2 reports;
- Regular meetings to discuss performance; and,
- Non-disclosure agreements.

The table below describes the subservice organizations used by C2FO.

<table>
<thead>
<tr>
<th>Control Activity Expected to be Implemented by Subservice Organization</th>
<th>Subservice Organization</th>
<th>Applicable Trust Services Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to data and software is restricted to authorized personnel.</td>
<td>● Amazon Web Services (AWS)</td>
<td>CC6.1</td>
</tr>
<tr>
<td></td>
<td>● Google Cloud Platform (GCP)</td>
<td></td>
</tr>
<tr>
<td>Physical access to the data center facility is restricted to authorized personnel.</td>
<td>● Amazon Web Services (AWS)</td>
<td>CC6.4</td>
</tr>
<tr>
<td></td>
<td>● Google Cloud Platform (GCP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Cavern Technologies</td>
<td></td>
</tr>
<tr>
<td>Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.</td>
<td>● Amazon Web Services (AWS)</td>
<td>A1.2</td>
</tr>
<tr>
<td></td>
<td>● Google Cloud Platform (GCP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Cavern Technologies</td>
<td></td>
</tr>
<tr>
<td>Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.</td>
<td>● Amazon Web Services (AWS)</td>
<td>A1.3</td>
</tr>
<tr>
<td></td>
<td>● Google Cloud Platform (GCP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Cavern Technologies</td>
<td></td>
</tr>
</tbody>
</table>