C2FO®

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

SOC 3SM Report

For the Period July 1, 2018 to June 30, 2019

SOC 3 is a registered service mark of the American Institute of Certified Public Accountants (AICPA)

BARR ADVISORY

Independent Service Auditor's Report

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

We have examined management's assertion that C2FO, during the period of July 1, 2018 through June 30, 2019, maintained effective controls to provide reasonable assurance that:

- the C2FO System was protected against unauthorized access, use, or modification to meet C2FO's commitments and system requirements
- the C2FO System was available for operation and use to meet C2FO's commitments and system requirements
- the C2FO System processing was complete, valid, accurate, timely, and authorized to meet C2FO's commitments and system requirements

based on the criteria for security, availability, and processing integrity in the American Institute of Certified Public Accountants' (AICPA) TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria). This assertion is the responsibility of C2FO management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included (1) obtaining an understanding of C2FO's relevant security, availability, and processing integrity controls; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions based on our findings to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls, or a deterioration in the degree of effectiveness of the controls.

In our opinion, C2FO's management assertion referred to below is fairly stated, in all material aspects, based on the aforementioned criteria for security, availability, and processing integrity.

BARR Advisory, P.A.

Fairway, KS

August 19, 2019

C2FO's Assertion on the Description of the C2FO System

C2FO maintained effective controls over the security, availability, and processing integrity of its C2FO System to provide reasonable assurance that:

- the C2FO System was protected against unauthorized access, use, or modification to meet C2FO's commitments and system requirements
- the C2FO System was available for operation and use to meet C2FO's commitments and system requirements
- the C2FO System processing was complete, valid, accurate, timely, and authorized to meet C2FO's commitments and system requirements

during the period February 1, 2019 through May 31, 2019, based on the criteria for security, availability, and processing integrity principles set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

Our attached "C2FO's Description of Its C2FO System" identified the aspects of the C2FO System covered by our assertion.

Subservice providers are used to perform data center, infrastructure, software, and managed hosting services.

Pollen, Inc.

August 19, 2019

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 (English, French, Spanish, German, Chinese/Cantonese);
- 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;
- 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,
- The end-to-end process for a buyer's market launch averages 8-12 weeks, while the technology initiative averages 3-4 weeks.

For suppliers specifically

Simple connection:

- No software download required, nor integration with existing tools; and,
- Mobile app and desktop view of the market.

Principal Service Commitments and System Requirements

C2FO designs its processes and procedures related to the C2FO system to meet its objectives. Those objectives are based on the service commitments that C2FO makes to user entities, the laws and regulations that govern the provision of the 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:

- Security principles within the fundamental designs of the C2FO system that 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.
- 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.
- Use of boundary protection systems, including web application firewalls (WAF), 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.
- 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.
- 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 client-server 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 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.
        - The cluster sits behind load balancers, which distribute website traffic across site servers.
        - User interactions with the web frontend trigger RESTful calls to the supporting infrastructure servers.
        - These servers perform business logic interactions with the C2FO database, where data access and manipulation is required.

    b. **Admin Webapp:** This portion is structured in the same way as the web portal, but with higher-privileged access for C2FO to monitor, 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 C2FO and buyers as follows:
    a. Raw data such as invoices, organizations, divisions, and user information from buyers are 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 could 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 elected to upload to S3 already, it is copied from the S3 bucket to one that can only be accessed by C2FO users and services.

    d. A timed service checks for buyer files. 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 MongoDb, where they are later aggregated and stored to the C2FO database for review by the C2FO webapp admin 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 buyers' 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. Stats: This service gathers system statistics and compiles it 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 EU may log in from the United States. That user's credentials are still stored in 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 General Data Protection Regulation (GDPR). These requirements are satisfied in the following manner:

a. A user's email and password are stored in the datacenter, 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 datastore of the eSLAP file that was uploaded. Information for supplier users who self-register is directed to and stored in the nearest IaaS and region by the API Gateway.

b. In order 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 request 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 uses a tool called Frenzy to manage its software deployments. Frenzy was created in-house as a way to use Docker containers to ensure that software builds are consistent across environments. Users with the correct permissions can use the web interface to deploy a range of build types as defined by source-controlled AWS CloudFormation files for AWS deployments, and through a combination of Ansible and manual procedures for GCP deployments. Frenzy accounts are managed with Windows Active Directory.

Achieving Scalability

Scalability is of critical importance to C2FO. C2FO follows service-oriented 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. C2FO internal users are authenticated via C2FO 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 is using Cavirin to scan both infrastructure and service hosts for known security vulnerabilities and bad practices.

Monitoring Performance, Scalability, and Availability

Performance monitoring in C2FO is done using DataDog, Pingdom, Sumo Logic, and Stackdriver. 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 200 employees headquartered in the Leawood, KS, office. C2FO has other offices at the following locations: Seattle, San Francisco, London, Frankfurt, Amsterdam, Singapore, and Hong Kong.

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 and procedures used to safeguard C2FO systems and data include:

- Security Awareness and Training Policy;
- Personnel Security Policy;
- Access Control Policy;
- Physical and Environmental Protection Policy;
- Risk Assessment Policy;
- Data Lifecycle Management Policy;
- Change Management Policy;
- Vendor Management Policy;
- Incident Management Policy;

- Vulnerability Management Policy;
- Data Retention Policy;
- Mobile Device Management Policy;
- Social Media and Internet Usage Policy;
- Clean Desk Policy;
- Information Security Policy;
- Personally Identifiable Information Policy;
- Log Policy;
- Security Committee Charter;
    - Security Committee Charter Attestation
- Bring Your Own Device Policy;
- Cookie Usage Policy;
- Visitor Policy;
- Encryption and Key Management Policy;
- Clock Synchronization Policy;
- Customer Password Reset Policy;
- Teleworking Policy;
- Associate Onboard and Offboard Policy; and,
- Business Continuity and Disaster Recovery Plan.

Data

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

- Invoices;
- Users;
- Organizations; and,
- 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 either Amazon RDS or Google Compute Engine Postgres instances, depending on the infrastructure provider, and is encrypted at rest. Access to the databases is strictly limited based on user roles. User accounts are managed with AWS and GCP Identity Access Management (IAM).

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 communications 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.
- 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,
- Nondisclosure agreements.

The table below describes the subservice organizations used by C2FO.

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Trust Services Criteria
Access to data and software is restricted to authorized personnel.	• Amazon Web Services (AWS) • Google Cloud Platform (GCP)	CC6.1
Physical access to the data center facility is restricted to authorized personnel.	• Amazon Web Services (AWS) • Google Cloud Platform (GCP) • Cavern Technologies	CC6.5
Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	• Amazon Web Services (AWS) • Google Cloud Platform (GCP) • Cavern Technologies	CC6.5 A1.2
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.	• Amazon Web Services (AWS) • Google Cloud Platform (GCP) • Cavern Technologies	A1.3

