# Kalderos, Inc.
# Chicago, Illinois

## System and Organization Controls Report Relevant to the Discount Monitoring and 340B Pay Solutions System

## SOC 3® Report

November 1, 2020 to October 31, 2021

*The report, including the title page, table of contents, and sections, constitutes the entire report and should be referred to only in its entirety and not by its component parts. The report contains proprietary information and is considered confidential.*

**Kalderos, Inc.**

**SOC 3 Report**
**November 1, 2020 to October 31, 2021**

# Table of Contents

# Section 1
# Kalderos, Inc.’s Assertion

## Kalderos, Inc.’s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Kalderos, Inc.’s (“Kalderos”) Discount Monitoring and 340B Pay Solutions System (the “system”) throughout the period November 1, 2020 to October 31, 2021, to provide reasonable assurance that Kalderos’s service commitments and system requirements relevant to security,  processing integrity, and confidentiality were achieved.  Our description of the boundaries of the system is presented in Attachment A and identifies 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 November 1, 2020 to October 31, 2021, to provide reasonable assurance that Kalderos’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (the “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*).  Kalderos’s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria.  The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B**.**

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

We assert that the controls within the system were effective throughout the period November 1, 2020 to October 31, 2021, to provide reasonable assurance that Kalderos’s service commitments and system requirements were achieved based on the applicable trust services criteria.

# Section 2
# Independent Service Auditor’s Report

WIPFLI

# Independent Service Auditor’s Report

Management of Kalderos, Inc.
Chicago, Illinois

### *Scope*

We have examined Kalderos, Inc.’s (“Kalderos”) accompanying assertion titled "Kalderos, Inc.’s Assertion" (the “assertion”) to determine that the controls within Kalderos’s Discount Monitoring and 340B Pay Solutions System (the “system”) were effective throughout the period November 1, 2020 to October 31, 2021, to provide reasonable assurance that Kalderos’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, processing integrity, and confidentiality (the “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*

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

### *Service Auditor’s Responsibilities*

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

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 Kalderos’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 Kalderos’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.

# Independent Service Auditor’s Report (Continued)

### *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 Kalderos’s Discount Monitoring and 340B Pay Solutions System were effective throughout the period November 1, 2020 to October 31, 2021, to provide reasonable assurance that Kalderos’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Wipfli LLP

Wipfli LLP

Minneapolis, Minnesota
December 3, 2021

# Attachment A – Description of the Boundaries of Kalderos, Inc.’s Discount Monitoring and 340B Pay Solutions System

# Attachment A – Description of the Boundaries of Kalderos, Inc.'s Discount Monitoring and 340B Pay Solutions System

## Kalderos Inc. Overview

Kalderos was founded in 2016 by Jeremy Docken, Jim Bonkowski, and David DeVogel. Kalderos completed its Series B investment round in the second quarter of 2020. Kalderos has offices in Chicago, Illinois, and Brookfield, Wisconsin.

Kalderos is building unifying technologies that bring transparency, trust, and equity to the entire healthcare community. The mission is to solve systemic problems of the healthcare system, redefining how the business of healthcare performs. Kalderos delivers technology that solves the challenges facing the U.S. healthcare system in the drug discount space. Kalderos's solutions interface with healthcare providers, drug manufacturers, payers, and government agencies alike to increase transparency and restore trust—enabling everyone to focus on improving the health of people.

### Solutions

Discount Monitoring: Kalderos's discount monitoring solution allows providers and manufacturers to work together to identify past noncompliant discounts with an industry-leading algorithm trained on the nation's single largest labeled dataset related to duplicate discounts. This discount identification involves collaborative work with thousands of providers, all 50 states, and others to encourage a smooth resolution of noncompliant discounts.

340B Pay: Kalderos's 340B Pay solution sits at the center of providers, manufacturers, and payers, enabling all parties to manage 340B rebates at the point of sale through a central location. Kalderos all but eliminates noncompliant discounts by providing the right discount to the right party on the right transaction℠ from the moment of purchase.

### Tools

Review: Kalderos Review is an easy-to-use tool that allows manufacturers to work with 340B covered entities in good faith to verify suspected duplicate discounts.

Request: Kalderos Request is a secure and intuitive tool that enables providers to request drug discounts at the point of sale.

Verify: Kalderos Verify is a secure and intuitive tool designed to enable manufacturers to approve or fail discount requests submitted through the Request tool. Verify includes the Report Center (formerly known as Verify Report Center [VRC]) and the soon-to-be-added Dispute Center.

Avenue: Avenue is the legacy Kalderos reporting tool currently in production (Q4 2021) that supports the requirement manufacturers have to monitor their 340B, MDRP, and CMC rebate flows. In 2021-2022, that functionality is completely moving to Verify, and when the move is complete, Avenue will be retired.

### Infrastructure

The Verify, Request, Review, and Avenue Web Applications are hosted at Microsoft Azure ("Azure") data centers, using the Azure Infrastructure-as-a-Service (IaaS) offering. The various services making up the runtime and provisioning systems for the Verify, Request, Review, and Avenue web applications are deployed in multiple Azure U.S. regions, primarily the north central United States.

# Attachment A – Description of the Boundaries of Kalderos, Inc.’s Discount Monitoring and 340B Pay Solutions System

## Organizational Structure

Kalderos’s organizational structure has been designed to streamline decision making and empower teams to rapidly take action. Each team function has key responsibilities to help Kalderos build unifying technologies that bring transparency, trust, and equity to the entire healthcare community:

- Executive Team
- Product and Design
- Technology
- Business Operations and Growth
- Delivery Management
- Advanced Analytics
- Customer Operations
- Sales
- Brand and Marketing
- Information Security
- People
- Finance

Kalderos’s Board of Directors meets quarterly to review the current state of the business and performance against key strategic initiatives. The Executive Team sets strategic operational objectives at least annually, and these are then reviewed and approved by the Board of Directors at the annual session. Major corporate initiatives are codified and communicated to the entire Kalderos team through the use of the Objectives and Key Results (OKR) framework. Progress on major strategic initiatives is tracked regularly and is evaluated at least quarterly by the Board of Directors.

## Policies and Procedures

Kalderos maintains a policy management program to help ensure policies, procedures, and internal controls:

1. Are properly communicated throughout the organization.
2. Are properly owned, managed, and supported.
3. Clearly outline business objectives.
4. Show commitment to meet regulatory obligations.
5. Are focused on continual iteration and improvement.
6. Provide for an exception process.
7. Support the policy framework and structure.
8. Are a means to report policy noncompliance.

### Policy Requirements

Every policy has a policy owner who is responsible for managing the internal controls associated with the policy. All policies are reviewed at least annually to help ensure they are relevant and appropriately manage risk in accordance with Kalderos’s risk appetite. Changes are reviewed by the Information Security team and approved by the corresponding policy owner.

## Policies and Procedures (Continued)

Policy Requirements (Continued)

All active Kalderos policies are posted on the policy management platform and made available to Kalderos's employee community for training, acceptance, and future reference.

## Subservice Organizations

Kalderos uses subservice organizations to perform a range of functions.  The following describes the subservice organizations used by Kalderos:

| Subservice Organization | Function |
|---|---|
| Microsoft Azure | Cloud-based IaaS |
| Google G Suite | Communication, productivity, and collaboration services |
| Snowflake | Cloud data warehouse platform |
| Dwolla | Secure third-party payments platform |

## Complementary Subservice Organization Controls

Kalderos's controls related to the Kalderos Discount Monitoring and 340B Pay Solutions System cover only a portion of overall internal control for each user entity of Kalderos.  It is not feasible for the trust services criteria related to the Kalderos Discount Monitoring and 340B Pay Solutions System to be achieved solely by Kalderos.  Therefore, each user entity's internal control must be evaluated in conjunction with Kalderos's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization(s) as described below.

| Complementary Subservice Organization Controls |
|---|
| Procedures have been established to restrict physical access to the data center to authorized employees, vendors, contractors, and visitors. |
| Security verification and check-in are required for personnel requiring temporary access to the interior data center facility, including tour groups or visitors. |
| Physical access to the data center is reviewed quarterly and verified by the Data Center Management team. |
| Physical access mechanisms (e.g., access card readers, biometric devices, mantraps/portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals. |
| The data center facility is monitored 24/7 by security personnel. |
| External access to Azure, Google, and Snowflake services and the customer data stored in those services requires authentication and is restricted based on customer configured authorization settings. |
| Customer credentials used to access Azure and Dwolla services meet the applicable password policy requirements. |

# Attachment A – Description of the Boundaries of Kalderos, Inc.’s Discount Monitoring and 340B Pay Solutions System

## **Complementary Subservice Organization Controls** (Continued)

| Complementary Subservice Organization Controls |
|---|
| Logical segregation is implemented to restrict unauthorized access to other customer tenants. |
| Customer data that is designated as confidential is protected while in storage within Azure, Google, and Snowflake services. |
| Service initializes the resource groups in the management portal based on the customer-configured templates. |
| Customer data communicated through Azure, Google, Snowflake, and Dwolla service interfaces is encrypted during transmission over external networks. |
| Internal communication among key Azure, Google, Snowflake, and Dwolla components when customer data is transmitted/involved is secured using encryption. |
| Cryptographic controls are used for information protection within the Azure, Google, Snowflake, and Dwolla platforms based on cryptographic policy and key management procedures. |
| ACH payments via Dwolla API from partner manufacturers to discount recipients are managed for completeness, accuracy, and timeliness. |

# Attachment B – Service Commitments and System Requirements of Kalderos, Inc.'s Discount Monitoring and 340B Pay Solutions System

# Attachment B – Service Commitments and System Requirements of Kalderos, Inc.’s Discount Monitoring and 340B Pay Solutions System

## Principal Service Commitments and System Requirements

Kalderos designs its processes and procedures to address noncompliant drug discounts that have occurred in the past and help ensure drug discount compliance in the future to meet its objectives to build technology solutions to solve challenges facing the U.S. healthcare system in the drug discount space. Those objectives are based on the service commitments Kalderos makes to user entities, the laws and regulations that govern the provision of drug discount management technology services, and the financial, operational, and compliance requirements Kalderos has established for the services. Kalderos ‘s services are subject to (but not required at this time) the security and privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA), as well as state privacy security laws and regulations in the jurisdictions in which Kalderos operates.

Security, processing integrity, and confidentiality commitments to user entities are documented and communicated in master service agreements and other customer agreements, as well as in the description of the service offering provided online.

- Security commitments include principles within the fundamental designs of the solution that are designed to permit system users to access the information they need based on their roles in the system, while restricting them from accessing information not needed for their role.
- Processing integrity commitments include accuracy and consistency of data in the data life cycle.
- Confidentiality commitments include the use of encryption technologies to protect customer data both at rest and in transit.

Kalderos establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Kalderos’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 related to how the technology is designed and developed, the system is operated, the internal business systems and networks are managed, and employees are hired and trained. In addition to these policies, standard operating procedures on how to carry out specific manual and automated processes required when providing drug discount management technology have been documented.