System and Organization Controls (SOC) 3 Report

Management's Report of Its Assertions on Pre-Paid Legal Services, Inc. and EAP, Inc. dba CLC Legal and Identity Theft Services and CLC Application Systems Based on the Trust Services Criteria for security, availability and confidentiality

For the Period April 1, 2024 to January 31, 2025

TABLE OF CONTENTS

SECTION ONE: REPORT OF INDEPENDENT ACCOUNTANTS

To: Management of Pre-Paid Legal Services, Inc. and EAP, Inc. dba CLC

Scope

We have examined Pre-Paid Legal Services, Inc.'s and EAP, Inc.'s dba CLC ("PPLSI") accompanying assertion titled "Assertion of Pre-Paid Legal Services, Inc.'s and EAP, Inc.'s dba CLC Management" and MIDCON Recovery Solutions, Inc.'s ("Inclusive Subservice Organization" or "MIDCON") accompanying assertion titled "MIDCON Recovery Solutions, Inc.'s Assertion" (assertion) that the controls within PPLSI's Legal and Identity Theft Services and CLC Application Systems (system) were effective throughout the period April 1, 2024 to January 31, 2025, to provide reasonable assurance that PPLSI's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentilaity (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, *(With Revised Points of Focus—2022)* in AICPA *Trust Services Criteria.*

MIDCON is a subservice organization providing data center hosting services to PPLSI. The description of the boundaries of the system presented in Attachment A describes the data center hosting services provided to PPLSI and operated by MIDCON that are necessary for PPLSI to achieve its service commitments and system requirements based on the applicable trust services criteria.

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

Service and Subservice Organization's Responsibilities

PPLSI 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 PPLSI's service commitments and system requirements were achieved. PPLSI and MIDCON have also provided the accompanying assertion about the effectiveness of controls

within the system. When preparing its respective assertions, PPLSI and MIDCON are responsible for selecting and identifying in the 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 AICPA. 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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 PPLSI'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 PPLSI'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 PPLSI's Legal and Identity Theft Services and CLC Application Systems were effective throughout the period April 1, 2024 to January 31, 2025, to provide reasonable assurance that PPLSI's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

CyberGuard Compliance, LLP

August 20, 2025
Las Vegas, Nevada

SECTION TWO: MANAGEMENT'S REPORT OF ITS ASSERTIONS ON THE EFFECTIVENESS OF ITS CONTROLS OVER PRE-PAID LEGAL SERVICES, INC.'S AND EAP, INC.'S DBA CLC'S LEGAL AND IDENTITY THEFT SERVICES AND CLC APPLICATION SYSTEMS BASED ON THE TRUST SERVICES CRITERIA FOR SECURITY, AVAILABILITY AND CONFIDENTIALITY

August 20, 2025

Scope

We are responsible for designing, implementing, operating, and maintaining effective controls within Pre-Paid Legal Services, Inc.'s and EAP, Inc.'s dba CLC's (PPLSI) Legal and Identity Theft Services and CLC Application Systems (system) throughout the period April 1, 2024 to January 31, 2025, to provide reasonable assurance that PPLSI's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentilaity (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, *(With Revised Points of Focus—2022)* in AICPA *Trust Services Criteria.* Our description of the boundaries of the system is presented in Attachment A (description) and identifies the aspects of the system covered by our assertion.

MIDCON is a subservice organization providing data center hosting services to PPLSI. The description of the boundaries of the system presented in Attachment A describes the data center hosting services provided to PPLSI and operated by MIDCON that are necessary for PPLSI to achieve its service commitments and system requirements based on the applicable trust services criteria.

PPLSI uses a subservice organization to provide cloud hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at PPLSI, to achieve PPLSI's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2024, to January 31, 2025, to provide reasonable assurance that PPLSI's service commitments and system requirements were achieved based on the applicable trust services criteria. PPLSI'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 April 1, 2024, to January 31, 2025, to provide reasonable assurance that PPLSI's service commitments and system requirements were achieved based on the applicable trust services criteria.

Pre-Paid Legal Services, Inc. and EAP, Inc. dba CLC

MIDCON RECOVERY SOLUTIONS, INC.'S ASSERTION

August 20, 2025

We are responsible for effectively operating a portion of controls within Pre-Paid Legal Services, Inc.'s and EAP, Inc. dba CLC's (PPLSI) Legal and Identity Theft Services and CLC Application Systems (system) throughout the period April 1, 2024 to January 31, 2025, to provide reasonable assurance that PPLSI's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentilaity (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, *(With Revised Points of Focus—2022)* in AICPA *Trust Services Criteria.* The description of the boundaries of the system is presented in Attachment A (description) and identifies the aspects of the system covered by our assertion.

We assert that the portion of controls that we operated within the system were effective throughout the period April 1, 2024, to January 31, 2025, to provide reasonable assurance that PPLSI's service commitments and system requirements were achieved based on the applicable trust services criteria.

MIDCON Recovery Solutions, Inc.

ATTACHMENT A: PRE-PAID LEGAL SERVICES, INC.'S AND EAP, INC. DBA CLC'S DESCRIPTION OF THE BOUNDARIES OF ITS LEGAL AND IDENTITY THEFT SERVICES AND CLC APPLICATION SYSTEMS

Company Background

Founded in 1972 in Ada, Oklahoma, Prepaid Legal Services, Inc. (PPLSI) is the only carrier who specializes and offers a proprietary service that provides a legal (LegalShield) and identity theft solution (IDShield). PPLSI markets its products through three main business channels: 1. Business-to-Business, 2. Direct to Consumer and 3. Network Marketing.

Today, we're continuing to make an impact and empowering over 4.5 million individuals, 140,000 businesses, 40,000 employers, and 1.7 million people through their employers across North America and Canada to be legal-ready. With LegalShield, participants are provided direct access to a dedicated provider law firm. IDShield, LegalShield's identity theft and online privacy protection benefit, provides identity, credit, social media as well as financial account monitoring in addition to consultation and full-service restoration services. Restoration services are completed by a team of dedicated licensed private investigators.

The PPLSI's corporate operation is headquartered in Ada, Oklahoma, with one remote call center located in Duncan, OK and third-party call centers utilized within the US and Canada. The headquarters facility consists of a 177,000 square foot, state-of-the-art complex that houses all operational departments supporting membership application entry and related processing. The facility houses call centers handling customer service for members and associates, including staff responsible for commission payments, receipt of membership fees, general ledger accounting, human resources, internal audit, and a department that manages and monitors provider law firm relationships. The IT data centers are in the headquarters facility and at a third-party colocation facility in Oklahoma City, Oklahoma. PPLSI uses internal IT expertise and follows internal business and IT policies and procedures to support its daily IT administration and service operation.

System Overview

The System is comprised of the following components:

- ***Infrastructure*** **-** The physical and hardware components of a system (facilities, equipment, and networks)
- ***Software*** **-** The programs and operating software of a system (systems, applications, and utilities)
- ***Data*** **-** The information used and supported by a system (transaction streams, files, databases, and tables)
- ***People*** **-** The personnel involved in the operation and use of a system (developers, operators, users, and managers)

- ***Procedures*** **-** The automated and manual procedures involved in the operation of a system

Infrastructure

The IT network operates on a Microsoft Windows-based platform, using IBM client access to connect to their proprietary Customer Relationship Management software on the IBM System i. The IBM System i also houses a DB2 database that is the primary data store for the business. For security and redundancy purposes, multiple servers are used for various service delivery functions and applications.

PPLSI's infrastructure consists of two IBM Power Systems, one at each data center location. These servers support the core business applications and databases with real-time replication between the systems. In addition, there are a number of cloud services and virtual machines supporting various functions. Employees use desktop PCs, laptops running Windows and macOS productivity applications, and as well as Power Systems terminal emulation on a Windows server network.

- One Primary Database server and one Backup Database server
- Multiple Web servers
- Multiple Domain Control servers
- Security servers are deployed for intrusion detection, centralized logging, application scanning, device scanning and file integrity
- F5 and Fortinet Firewalls deployed
- Talkdesk Cloud Based Contact Center Solution

Software

The business develops critical applications in-house, which are supported by internal staff and contractors. These applications include member application entry, commissions, cash receipts, credit card processing, electronic bank draft, premium billing, claims, customer relationship management, web sites, mobile, group sites, and intake management administration for provider attorneys. Applications and critical business data are hosted in a hybrid hosting model.

PPLSI uses multiple software and utilities to configure, develop, and support the in-scope infrastructure and applications, including:

- CodeFresh – CI/CD Vendor
- Puppet - Software Config and Management Tool (industry standard, everyone uses this)
- Terraform - Cloud Config, deploy and management tech (about half the industry uses this)
- Docker – Container engine
- AWS - Elastic Container Registry – Container image repository

- GitHub – Online source code control repository and Package Registry

Data

All information is stored on PPLSI servers located in the United States. Information is treated as an asset that must be protected against loss and unauthorized access. Procedural and technical safeguards are in place to protect personal information against loss or theft as well as unauthorized access and disclosure. Security technologies are utilized to protect information from unauthorized access inside and outside of PPLSI.

Extended Validation Secure Socket Layer certificates are in use when personal information is uploaded or viewed on the PPLSI website. Each associate and member have a unique username and password that must be entered every time a user logs on to the website. Firewalls and layered security technologies prevent interference or access from outside intruders. The website is hosted on servers located in a secure data center.

PPLSI collects non-public personal information from the following sources:

- Information that is received from applications or other forms such as name, address, social security number, and payment instructions.
- Information that is provided during visits to the PPLSI web site or calls to customer service representatives.
- Information about customers' transactions with PPLSI, its affiliates or others.

PPLSI does not disclose non-public personal information about customers or former customers to non-affiliated entities except as described below and otherwise permitted by law. PPLSI may disclose information collected, as described above, to Provider Law Firms and companies that assist in the servicing or administration of the product that has been requested and authorized.

When information is shared with companies that perform services on behalf of PPLSI, PPLSI protects against the subsequent disclosure of that information with a confidentiality agreement.

People

The following functional roles/teams comprise the framework to support effective controls over governance, management, security, and operation:

Warren Schlichting, Chief Executive Officer (CEO), was named CEO of PPLSI in December 2022. Schlichting began his career with Morgan Stanley in their M&A group and served in executive positions at the William E. Simon private equity group. He has served in many top executive positions in several publicly and privately held companies such as Comcast, Sling TV and DISH. Other areas of service include a three-year stint as CEO of Hiwire, a Los Angeles-based Internet ad technology start-up, and six years as CEO of Yucatan Foods, a

venture he co-founded, advised and recently sold. He co-founded Camden Asset Management, a convertible arbitrage hedge fund, and has served on a number of company boards. Most recently, he served as Executive Vice President and Chief Operating Officer at Poly, formerly Plantronics and Polycom. Schlichting has received numerous industry awards and is a frequent keynote speaker and guest panelist. An annual selection to the *Cable Top 100 Heavy hitters* and two-term Board member of the Interactive Advertising Bureau (IAB), he also served on the board of Invidi, a data-driven ad-technology joint venture he championed between DISH and DirecTV. At present he is an advisor to Konvoy Ventures, an esports venture capital fund. Schlichting currently serves on the Board of the Boys & Girls Clubs of Metro Denver and prior to that helped found the Philadelphia chapter of Summer Search, an organization dedicated to providing mentoring and summer experiences to kids for whom these would be otherwise unattainable. Schlichting enjoys time with his family, is an avid fisherman, slow biker and enthusiastic golfer.

Ogemdi Ike, Chief Operations Officer, Ogemdi joined the Company in 2024. He brings a wealth of experience and expertise as a leader of customer and sales operations for Fortune 250 subscription-based companies. Prior to LegalShield, he was the Vice President of Sales Operations & Business Planning at T-Mobile. He's also held senior leadership roles at Experian and Omni Channel. His early career included management consulting and advisory assignments with Ernst & Young, KPMG, and Andersen Consulting.

Ogemdi has an MBA from the UNC's Kenan-Flagler Business School and a BA in engineering physics from Obafemi Awolowo University, in Ile-Ife, Nigeria.

Steve Williamson, EVP, Chief Financial Officer (CFO), serves as the Chief Financial Officer for PPLSI. Prior to joining the company, he was the CFO for Peripheral Enhancements, Inc. from April 1997 to March 2000. Steve served as Director in Charge of Banking Practice for Horne & Company, a public accounting firm, from November 1983 to April 1997. After graduating from East Central University in 1982, he began his career with the international accounting firm KPMY. Steve joined PPLSI as Chief Financial Officer in 2000. He is a Certified Public Accountant (CPA) and is a past board member and banking committee chair of the Oklahoma Society of CPAs.

Darnell Self, EVP of Network & Business Development, after earning a degree in public relations at Bowie State University, Darnell Self joined PPLSI in 1998. He has shared his vast experience in team building, personal development, and entrepreneurship since day one. These experiences allowed Mr. Self to orchestrate a duplicable system, garnering recognition in numerous business publications and the esteemed title of Entrepreneur of the Year by the National Black Chamber of Commerce. He is also a mentor to thousands of thriving entrepreneurs and has been asked to share his expertise with business students on several university platforms. Coming from humble beginnings, Mr. Self has

devoted his time and efforts to give people, no matter the circumstance, an opportunity to actualize their own success. This level of commitment has resulted in dozens of PPLSI Ring Earners and over a dozen Millionaire Club Members. Mr. Self and his colleague Michael Humes also collaborated to create Fertile Ground – an organization designed to allow others to experience the power of giving.

Mark Conlin, Chief Technology Officer, Mark has over 20 years of experience in software engineering as an IC and a leader and has worked in consulting firms, start-ups, and large global enterprises. Mark has led engineering teams through acquisition and scaling inside global enterprises, the modernization of legacy technology, and built software teams and products from the ground up. Most recently, Mark was responsible for marketplace engineering at Outdoorsy. Before that, he was the Travel and Commerce Platform owner with BCD Travel. His engineering and product teams powered hundreds of thousands of outdoor vacations and enabled billions in corporate travel bookings. Mark holds multiple degrees (Computer Science and MBA) from the Georgia Institute of Technology.

Don Thompson, President of Network Division, joined PPLSI in 1996 as an Independent Associate. During his career as an associate, Mr. Thompson has earned many top achievements, business builder, and production awards. He has served in many field leadership positions including Regional Vice President of Florida, Business Vice President of Florida, Ohio, and Michigan, and most recently, Sr. Network Vice President of 26 states and 2 provinces of Canada. Mr. Thompson has mentored and trained thousands of associates by teaching the fundamentals of leadership and personal development. Don Thompson was named President of the Network Division in December 2018. He is a graduate of John Carroll University, Boler School of Business, with a degree in Business Administration. Don is married to Angela, and has two boys, Matthew, and David.

PPLSI is committed to equal opportunity of employment, and all employment decisions are based on merit, qualifications, and abilities. Employment-related decisions are not influenced or affected by an employee's race, color, nationality, religion, sex, marital status, family status, sexual orientation, disability, or age. PPLSI endorses a work environment free from discrimination, harassment, and sexual harassment.

Procedures

New Member and Group Accounts

PPLSI has a series of procedures to set up new member and group accounts that use its legal services and identity theft products, including:

- Set up new member accounts based on the type of plan purchased
- Set up secure data transfer for group accounts
- Set up individual authorized member users and group accounts for their web platform

Once new member accounts have been established within the system, the following activities occur to ensure services are performed accurately, completely, and timely:

- Member Services Representatives answer calls from members about services
- Quality assurance reviews Member Services calls
- Provider Services Representatives help members with complaints and referrals

The system has statistical information management tools for recording all services during the circle of the process workflow, including the services volume, services turnaround time. Additionally, the system has built-in audit trails for tracking all information alteration or correction activities. All system informational changes performed are recorded by the system with a time stamp.

Secure Access to Information Assets

PPLSI communicates the established security policies, user rights and responsibilities, and restrictions to the employees of the company. Management performs annual reviews of user access profiles and ensures that the appropriate people are assigned to those profiles. The number of employees that have administrator rights to hardware or applications is restricted.

Logs are reviewed to ensure that the use of administrative rights is appropriate. The setup, change, or elimination of user rights follows established procedures.

PPLSI performs intrusion detection testing. All firewall and networking hardware is reviewed for proper configuration and proper software levels. Firewall and network logs are reviewed for security events. Potential security or intrusion events are monitored on the network and servers. Remote access is restricted, controlled, and required to have security authentication before allowing access. Data that is sensitive is transmitted in a protected format, such as through a VPN or with appropriate levels of encryption.

Develop, Acquire, Implement, and Maintain Software

PPLSI has established procedures for the systems development lifecycle, project management, and change management to govern applications development and maintenance. These procedures are designed to facilitate an orderly development process with appropriate review, testing, and audit trails, ensuring segregation of duties between programmers and the production environment.

PPLSI reviews system events and activity logs. Processes are used to ensure system software is upgraded to assist in preventing security breaches. Software that is applied to systems is tested before implementation. A process exists to purchase software and track software licensing compliance after its purchase.

Complementary Subservice Organization Controls

Certain principal service commitments and system requirements can be met only if complementary subservice organization controls (CSOC) assumed in the design of PPLSI's controls are suitably designed and operating effectively at the subservice organization, along with related controls at PPLSI.

MIDCON

PPLSI uses MIDCON as the colocation facility for the production systems. The Complementary Subservice Organization Controls (CSOCs) identified at MIDCON were tested via the inclusive method, and are required, alone or in combination with controls at PPLSI, to provide assurance that PPLSI's service commitments and system requirements are achieved.

Through daily operational activities, PPLSI management and IT administration personnel monitor the services provided by MIDCON to ensure that operations and controls expected to be implemented are functioning effectively.

Amazon Web Services (AWS)

AWS provides the primary hosting infrastructure for the in scope systems, including compute, storage, and backup services. AWS is responsible for ensuring physical security, power redundancy, network availability, and data durability. PPLSI relies on AWS' controls for data center operations, geo-redundant backup storage, and platform availability.

PPLSI management reviews AWS' SOC 2 Type 2 report annually as part of its vendor risk management program. Any deficiencies identified in the report are evaluated for potential impact to AWS' services, users, and control environment.

Applicable Trust Services Criteria	Complementary Subservice Organization Control
6.4	AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including network devices and servers.
A 1.2	AWS is responsible for ensuring environmental protection controls are in place to meet availability commitments and requirements.

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Description of Services Provided

PPLSI markets two products: PPLSI and IDShield:

- **PPLSI** - Instead of paying a lawyer's expensive hourly fees, the customer pays a small monthly fee and gets access to experienced lawyers who can help them with their legal issue.
- **IDShield** – Protection of its customers' cybersecurity with identity and credit monitoring. IDShield not only alerts the customers about threats, but it also works for as long as it takes to restore its customers' identity.

Principal Service Commitments and System Requirements

PPLSI's security, availability, and confidentiality commitments to customers are documented and communicated to customers in the Associate and Member agreements. PPLSI security requirements are documented and published on the customer-facing website. Standard security, availability, and confidentiality commitments include, but are not limited to:

- Maintain appropriate administrative, physical, and technical safeguards to protect the security and integrity of the Information Technology platform and the customer data in accordance with PPLSI's security requirements.
- Perform regular security audits of the environment.
- Use formal HR processes, including background checks, code of conduct and company policy acknowledgements, security awareness training, disciplinary processes, and annual performance reviews.
- Follow formal access management procedures for the request, approval, provisioning, review, and revocation of PPLSI personnel with access to any production systems.
- Prevent malware from being introduced to production systems.
- Use industry-standard secure encryption methods to protect customer data at rest and in transit.
- Maintain a disaster recovery and business continuity plan to ensure availability of information following an interruption or failure of critical business processes.
- Maintain and adhere to a formal incident management process, including security incident escalation procedures.
- Maintain confidentiality of customer data and notify customers in the event of a data breach.

PPLSI regularly reviews security, availability, confidentiality, and performance metrics to ensure these commitments are met. If material changes occur that decrease the level of security, availability, or confidentiality commitments within the agreement, PPLSI will notify the customer directly.