System and Organization Controls (SOC) 3 Report

Management's Report of Its Assertions on LegalShield's Legal Services System Based on the Trust Services Criteria for Security, Availability and Confidentiality

For the Period December 1, 2019 to November 30, 2020

Independent SOC 3 Report for Security, Availability and Confidentiality Trust Services Criteria for LegalShield.

TABLE OF CONTENTS

SECTION ONE: REPORT OF INDEPENDENT ACCOUNTANTS

To: Management of Pre-Paid Legal Services, Inc. dba LegalShield

Scope

We have examined management's assertion, contained within the accompanying "Management's Report of Its Assertions on the Effectiveness of Its Controls over LegalShield's Legal Services System Based on the Trust Services Criteria for Security, Availability and Confidentiality" (Assertion) that LegalShield's controls over the legal services system (System) were effective throughout the period December 1, 2019 to November 30, 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (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*).

The Assertion also indicates that Pre-Paid Legal Services, Inc. dba LegalShield's ("Service Organization" or "LegalShield") controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of LegalShield's infrastructure's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

LegalShield uses a subservice organization to provide data center 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 LegalShield, to achieve LegalShield's service commitments and system requirements based on the applicable trust services criteria. Our examination included the services provided by the subservice organization, and we have evaluated the suitable design and operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

LegalShield management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the legal services system and describing the boundaries of the System;
- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of the System; and
- Identifying, designing, implementing, operating, and monitoring effective controls over the legal services system (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes:

- Obtaining an understanding of LegalShield's legal services system relevant to security, availability and confidentiality policies, procedures, and controls;
- Testing and evaluating the operating effectiveness of the controls; and
- Performing such other procedures as we considered necessary in the circumstances.

The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating LegalShield's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent Limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design and operating effectiveness of the controls to achieve LegalShield's legal services system's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system of controls, may alter the validity of such evaluations.

Opinion

In our opinion, management's assertion that the controls within LegalShield's legal services system were effective throughout the period December 1, 2019 to November 30, 2020 to provide reasonable assurance that LegalShield'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

April 12, 2021
Las Vegas, NV

SECTION TWO: MANAGEMENT'S REPORT OF ITS ASSERTIONS ON THE EFFECTIVENESS OF ITS CONTROLS OVER LEGALSHIELD'S LEGAL SERVICES SYSTEM BASED ON THE TRUST SERVICES CRITERIA FOR SECURITY, AVAILABILITY AND CONFIDENTIALITY

April 12, 2021

Scope

We, as management of LegalShield, are responsible for:

- Identifying our principal service commitments and system requirements (Attachment A);
- Identifying the LegalShield Legal Services System (System) and describing the boundaries of the System, which are presented in Attachment B below titled "LegalShield's Description of the Boundaries of Its Legal Services System";
- Identifying the risks that would threaten the achievement of our principal service commitments and service requirements that are the objectives of our system;
- Identifying, designing, implementing, operating, and monitoring effective controls over LegalShield's Legal Services System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements; and
- Selecting the trust services categories that are the basis of our assertion.

In designing the controls over the System, we determined that certain trust services criteria can be met only if complementary user entity controls are suitably designed and operating effectively for the period December 1, 2019 to November 30, 2020.

LegalShield uses a subservice organization to provide data hosting services. The description of the boundaries of the system indicate that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at LegalShield, to achieve LegalShield's service commitments and system requirements based on the applicable trust services criteria.

We assert that the controls within the system were effective throughout the period December 1, 2019 to November 30, 2020, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability and confidentiality set forth in the AICPA's TSP section 100, 2017 *Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy*, if user entities applied the complementary controls assumed in the design of LegalShield's Legal Services System controls throughout the period December 1, 2019 to November 30, 2020.

Pre-Paid Legal Services, Inc. dba LegalShield

ATTACHMENT A: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

LegalShield provides legal plans and identity theft solutions to families and small businesses across the U.S. and Canada. LegalShield markets its products through two main channels: Business-to-Business and Networking. Independent benefit brokers provide the products to corporate employees through payroll deduction. More than 35,000 companies offer LegalShield plans to their employees. With 1.75 million families enrolled, LegalShield's legal plans currently protect 4 million people in 50 U.S. states and Canadian provinces. LegalShield is the only national legal safeguard to provide its participants with access to quality legal services from an accomplished law firm in their state or province for legal advice and assistance no matter how trivial or serious the issue. For a low monthly fee, LegalShield participants get access to qualified attorneys who are experts in the areas of law that most impact families and small businesses. LegalShield provides dedicated provider law firms throughout the U.S. and Canada enabling participants to feel as though they have their own personal law firm to call for help without having to worry about high hourly rates. LegalShield identity theft plans have restored over 15,000 identities. Our identity theft plans provide more than just credit monitoring – we also provide consultation on any identity theft issue and complete identity restoration in the event an identity is stolen. We field more than two million calls each year. With over 700 LegalShield employees dedicated to serving our groups and their employees, our promise is to provide outstanding legal and identity theft services at an affordable price.

LegalShield's security commitments to customers are documented and communicated to customers in the Associate and Member agreements. LegalShield security and privacy requirements are documented and published on the customer-facing website. Standard security 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 LegalShield'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 LegalShield 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.

LegalShield 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, LegalShield will notify the customer directly.

ATTACHMENT B: LEGALSHIELD'S DESCRIPTION OF THE BOUNDARIES OF ITS LEGAL SERVICES SYSTEM

The boundaries of a system are the specific aspects of a service organization's infrastructure, software, people, procedures, and data necessary to provide its services. The boundaries of LegalShield's system include applications and infrastructure that directly support the services provided to LegalShield's members and associates. Applications, databases, and infrastructure that indirectly support the services provided to LegalShield's clients are not included within the boundaries of LegalShield's system.

The System is comprised of the following components:

- ***Network and 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

Network and 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.

LegalShield'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

- Cisco, F5, and Fortinet Firewalls deployed inline
- NICE/InContact Cloud Based Contact Center Solution

Physical Security

LegalShield's corporate operation is headquartered in Ada, Oklahoma, with marketing offices in Denver, CO and Brossard, QC, Canada and two remote call centers located in Duncan, OK and Antlers, OK. 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 located in the headquarters facility and in Oklahoma City, Oklahoma. LegalShield uses internal IT expertise and follows internal business and IT policies and procedures to support its daily IT administration and service operation.

Corporate Headquarters

Security guards and video cameras are present throughout the building grounds and within the building. The buildings and grounds are monitored 24 x 7. The first layer of physical security is the gate at the entrance to the property. Visitors are required to stop and check with the security guard at the main gate before gaining access to the parking area.

The second layer of physical security are the proximity card key readers, software and badges that control physical access to the buildings and all secured areas within the building. Off-hour access to the gate at the entrance to the property is controlled by card key access.

Restricting physical access ensures that our computing assets (servers, network, information, etc.) are not exposed to unwarranted risks. The third layer of physical security is the restriction of physical access to the information centers to only those staff members required to have access to complete their job functions. All other staff members and vendors are required to sign-in and must be escorted for the duration of their visit.

Primary Data Center

The primary data center is hosted at a third-party colocation facility. The following controls at this subservice organization were included in the scope of LegalShield's SOC 2 examination:

- Physical access to facilities is controlled with the use of electronic locks using access cards.
- Physical access to sensitive areas is restricted to authorized personnel.
- Visitors, including all contractors and vendors, must prove identity, sign a visitor log, and be escorted through non-public areas of the Company facility.
- Procedures are implemented to enforce controls around the management of removable media. The use of removable media is limited to those with a valid business need.

- Human Resources is responsible for notifying IT of terminated employees and contractors. IT terminates logical access within 24 hours of notification.
- Terminated employee and contractor access to Company facilities is removed upon termination and company assets returned.
- Annually, owners of sensitive areas of the facilities review a list of the names and roles of those granted physical access to their areas to verify for continued business need.

Logical Security

Security software and devices are used to protect against unauthorized access, destruction, disclosure or modification of information and applications programs. Logical access controls are layered and govern access to the network, servers, applications and information. Logical access to the network, servers, applications and information is restricted to only those staff members required to have access to complete their job functions.

All employees and contractors are required to login to the internal network first and authenticate, which is the first layer of logical security. Once network access has been authenticated, an internal user may login to servers or applications, which requires additional authentication and is the second layer of logical security. Access privileges for users are established via a standard authorized access request process and granted in accordance with job-related duties. LegalShield's Content Management System for corporate websites can be accessed directly from the web for authorized employees and contractors.

Systems are configured to maximize the enforcement of security. LegalShield uses proper user ID and password procedures to ensure security, and all users must have unique user IDs to gain access to systems.

Environmental Protections

Computer operations and servers are protected by the following safeguards and environmental control systems, both at the third-party colocation facility and the data center at LegalShield's corporate headquarters:

a. Smoke detectors
b. Fire alarm system
c. Raised floors
d. Climate conditioning
e. Emergency power-off
f. UPS including battery backup and diesel generator power
g. Automatic fire suppression system
h. Hand-held fire extinguishers
i. Water detectors
j. Temperature and humidity control devices

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 on premise.

People

Bios of key LegalShield Personal

Jeff Bell, Chief Executive Officer and Board of Directors, was named Chief Executive Officer of LegalShield in July, 2014, the leading provider of legal and identity theft protection services in the US and 4 Canada provinces. Since his arrival, LegalShield has grown to over 1.7 million members, protecting and empowering over 4 million lives. Previously, Mr. Bell was Corporate Vice President, Global Marketing, Xbox, for Microsoft Inc. from 2006 to 2009. He spent 12 years at Ford Motor Company, including serving as Managing Director of Ford Spain, and 5 years at Chrysler as the Vice President and General Manager of Chrysler and Jeep Divisions. Jeff earned the 2008 Cannes Grand Prix Winner for the Halo 3 Integrated Marketing campaign. He was named AdAge "2007 Entertainment Marketer of the Year" for Gears of War, and AdAge "2005 Interactive Marketer of the Year" at Chrysler. He has served as Trustee of his alma mater, Kenyon College, and on the Board of the National Multiple Sclerosis Society. Bell graduated from Kenyon College Magna Cum Laude, Phi Beta Kappa and was honored as an Academic All-American in football. He holds Master's degrees from Johns Hopkins and Wharton. He is married to his wife of 30 years, Colleen, and has three sons, Josh, Jon and Matt.

Kathy Pinson, EVP, Chief Operations Officer, currently serves as LegalShield's Chief Operating Officer, working with and supporting all Vice Presidents of LegalShield, coordinating all administrative functions within the home office and field operations. With the company since 1979, Kathy has served with distinction in a number of roles, including Controller, Board Member, Secretary/Treasurer, Vice President of Marketing Administration and Executive Vice President of Operations. Ms. Pinson is a Certified Public Accountant, and served more than 20 years managing the regulatory compliance division of the company.

Steve Williamson, EVP, Chief Financial Officer, has been with LegalShield for over 12 years. Prior to joining the company, he served as the Chief Financial Officer 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 KPMG. Since 2000, Steve has served as LegalShield's Chief Financial Officer. 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 LegalShield 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 LegalShield 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.

Keri C. Norris, EVP, Legal & Regulatory Affairs and General Counsel, joined LegalShield as its first General Counsel in 2003. She oversees the company's legal affairs, including litigation, corporate legal matters, and regulatory and governmental matters. She also serves as an advisor to the company's executive management team. Prior to joining LegalShield, she was an associate attorney at Crowe & Dunlevy in Oklahoma City and at Hunton & Williams in Raleigh, North Carolina, where she specialized in commercial litigation, intellectual property litigation, and creditor's rights and bankruptcy. Ms. Norris is a member of the Association of Corporate Counsel of America, American Bar Association, the Oklahoma and North Carolina Bar Associations and the Pontotoc County Bar Association. She serves on the American Bar Association Standing Committee on Group & Prepaid Legal Services and the Group Legal Services Association. She earned a B.A. (English) and a J.D., both summa cum laude, from Oklahoma City University.

Arnold Blinn, EVP, Chief Technology Officer, most recently Arnold was the Chief Product Architect at GoDaddy where he spent seven years helping to redefine the product architecture, integration, and technical strategy of the company. Prior to joining GoDaddy Arnold was a Partner Architect at Microsoft Corporation. He spent 17 years working on the Windows Phone, Xbox, Windows Live, and MSN in a variety of roles driving product teams and division level product architecture. He also ran several new product incubation teams during this time, including several domains and DNS related services that ultimately became parts of O365 and part of Azure. Before Microsoft Arnold was the co-founder of eShop, an early pioneer in online commerce and electronic shopping. This company was acquired by Microsoft in 1996 and formed the basis of Microsoft Commerce Server. Arnold has approximately 40 patents issued and another 40 pending in electronic commerce, digital rights management, photo manipulation, domains and other online services. He holds a B.S. degree in Mathematics (Computer Science) from Carnegie Mellon University. Arnold has also served as a visiting scholar and has served on the University and Department of Computer Science Alumni Advisory Boards at Carnegie Mellon University.

Glen Peterson, President of LegalShield Business Solutions, is President of LegalShield's Business Solutions division, responsible for business development, strategy and sales growth for LegalShield's affinity, broker, voluntary benefits, national accounts and small business divisions. He has 25 years of experience in the benefit space and is an industry expert in the worksite voluntary

benefits arena. Glenn previously served as SVP of LegalShield's Broker and Partnership Sales and was a VP at Metlife for nearly 10 years. He has managed and led many successful voluntary benefit sales organizations making him well-versed in voluntary benefits.

Don Thompson, President of Network Division joined LegalShield 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.

Cameron Scott, Chief Marketing Officer, joined LegalShield in 2020 and leads all aspects of LegalShield's global marketing strategy and execution, including brand and performance marketing, community engagement, product marketing and customer lifecycle management. Prior to joining LegalShield, Cameron was Chief Brand Officer at GoDaddy, where for nearly a decade he worked to evolve the company's brand as he led their advertising, creative, sponsorships, social and marketing communications teams. A technology pioneer for 25+ years, Cameron has been at the forefront of innovation, playing a key role in many digital tools and services that are now internet staples, including digital communications, online advertising, and massive-scale service platforms known collectively today as "the cloud." Before joining GoDaddy in 2013, Cameron held a variety of senior strategy and marketing roles at Microsoft, Yahoo! and AT&T Wireless. Cameron holds a BS in Political Science from Oregon State University and lives with his wife and young son in Seattle, Washington.

Martine Girotto, President of LegalShield Canada, with over 17 years experience in various roles and capacities, Martine brings a wealth of contribution and knowledge within the Direct Sales Industry. Prior to joining LegalShield, Martine served as General Manager of Canada at Jeunesse Global for 3 years, where she was responsible for the market strategy, sales, leadership development and marketing efforts in Canada. As well, with more than 10 years as Director of Sales at Mary Kay Cosmetics, Canada, Martine has developed a passion for the industry and her strong work ethics paired with her ability to balance strategy and tactics have allowed her to gain influence with field and corporate leaders alike. Her degree in psychology and her love for helping others, makes her a great asset for the Canadian market. Martine resides in Montreal with her husband of 18 years and their two sons. She is a proud football mom and has applied her leadership qualities in volunteering for over 7 years with football associations, while also teaching her children about the power of giving back.

Todd Barrs, VP of Direct to Consumer, joined LegalShield in 2018. Prior to joining the company, he served as VP of Ecommerce at multiple technology start-ups where he led numerous successful digital transformation initiatives. Todd has developed and implemented digital and eCommerce programs for a wide range of B2C and B2B organizations in the enterprise SaaS, software security,

telecom, online education, apparel and CPG industries. He is a nationally recognized speaker on the topics of digital strategy, web analytics and website testing. Todd holds an MBA from The George Washington University and a BS in Mechanical Engineering from Colorado State University.

Data

All information is stored on LegalShield 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 LegalShield.

Extended Validation Secure Socket Layer certificates are in use when personal information is uploaded or viewed on the LegalShield 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.

LegalShield 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 LegalShield web site or calls to customer service representatives.
- Information about your transactions with LegalShield, its affiliates or others.

LegalShield 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. LegalShield 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 LegalShield, LegalShield protects against the subsequent disclosure of that information with a confidentiality agreement.

In no event does LegalShield disclose personal information to companies that will use that information to contact you about their own products or services.

Procedures

New Member and Group Accounts
LegalShield 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
LegalShield 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.

LegalShield 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
LegalShield 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.

LegalShield reviews system event 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 LegalShield's controls are suitably designed and operating effectively at the subservice organization, along with related controls at LegalShield. The CSOCs at the third-party colocation facility are included in this description of the boundaries of the system and were included in the service auditor's examination of SOC 2 controls.

Complementary User Entity Controls

LegalShield controls were designed with the assumption that certain controls would be implemented by user entities (or "customers"). Certain requirements can be met only if complementary user entity controls assumed in the design of LegalShield's controls are suitably designed and operating effectively, along with related controls at LegalShield.