



## **SOC 3 Report**

**Report on LegalShield's Legal and Identity Theft Services System  
Relevant to Security, Availability, Processing Integrity, and Confidentiality  
for the Period of January 1, 2018 through November 30, 2018**



## I. INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of LegalShield  
Ada, Oklahoma

We have examined management's assertion that LegalShield (the "Company") maintained effective controls to provide reasonable assurance that:

- Its system was protected against unauthorized access, use, or modification to achieve the Company's commitments and system requirements;
- Its system was available for operation and use to achieve the Company's commitments and system requirements;
- Its system processing was complete, valid, accurate, timely, and authorized; and
- Information within its system is collected, used, disclosed, and retained to achieve the Company's commitments and system requirements.

during the period of January 1, 2018 to November 30, 2018, based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality ("applicable trust services criteria") set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Trust Services Criteria*).

The Company's management is responsible for its assertion. Our responsibility is to express an opinion based on our examination. Management's description of the aspects of the system covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA") and, accordingly, included (1) obtaining an understanding of the Company's controls relevant to the applicable trust services criteria; (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 the nature and inherent limitations of controls, the Company's ability to meet the applicable trust services criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, the Company's assertion referred to above is fairly stated, in all material respects, based on the applicable trust services criteria.



Dallas, Texas  
March 6, 2019

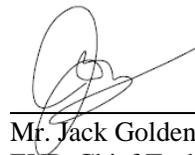
## II. MANAGEMENT OF LEGALSHIELD'S ASSERTION

We, as management of LegalShield (the "Company"), are responsible for designing, implementing, and maintaining effective controls over the Company's legal and identity theft services system to provide reasonable assurance that its commitments and system requirements are achieved. We have performed an evaluation of the controls over the Company's legal and identity theft services system for the period of January 1, 2018 to November 30, 2018 to achieve the Company's commitments and system requirements based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality ("applicable trust services criteria") set forth in TSP section 100A, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016) (AICPA, Trust Services Criteria).

Based on this evaluation, we assert that the Company's controls were effective for the period of January 1, 2018 to November 30, 2018 to provide reasonable assurance that:

- Its system was protected against unauthorized access, use, or modification to achieve the Company's commitments and system requirements;
- Its system was available for operation and use to achieve the Company's commitments and system requirements;
- Its system processing was complete, valid, accurate, timely, and authorized; and
- Information within its system is collected, used, disclosed, and retained to achieve the Company's commitments and system requirements.

Our attached description of the Company's legal and identity theft services system identifies the aspect of the Company's system covered by our assertion.



---

Mr. Jack Goldenberg  
EVP, Chief Technology Officer

### III. DESCRIPTION OF LEGALSHIELD'S LEGAL AND IDENTITY THEFT SERVICES SYSTEM

#### OVERVIEW OF OPERATIONS

Founded in 1972 in Ada, Oklahoma, LegalShield is a leading provider of 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 deductions. More than 34,000 companies offer LegalShield plans to their employees. With 1.75 million families enrolled, LegalShield's legal plans currently protect 4.375 million people in 50 U.S. states and four Canadian provinces. 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 pay hourly rates. LegalShield identity theft plans currently cover 1.7 million people with nearly 10,000 identities restored. With over 700 LegalShield employees dedicated to serving our groups and their employees, our goal is to provide outstanding legal and identity theft services at an affordable price.

Our corporate operation is headquartered in Ada, Oklahoma with offices in Oklahoma City, OK 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 of the 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.

#### OVERVIEW OF THE SYSTEM AND APPLICATIONS

##### *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); and
- **Procedures:** The automated and manual procedures involved in the operation of a system.

### III. DESCRIPTION OF LEGALSHIELD'S LEGAL AND IDENTITY THEFT SERVICES SYSTEM (continued)

#### Infrastructure

LegalShield's technology environment 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 PC's and laptops running Windows productivity applications and 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

#### 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 are hosted on premise and on cloud platforms including Heroku, Acquia, and AWS. Critical business data is hosted on premise.

#### People

**Jeff Bell, Chief Executive Officer** – He was named CEO in July 2014. Mr. Bell has over 20 years of corporate leadership and consumer marketing experience for global brands including Microsoft, Chrysler, Ford, and NBCUniversal. Most recently, he was the Chief Client Officer for vRide, the nation's leading provider of carpool and vanpool services. Under his leadership, Xbox created innovative, award-winning and multi-million-dollar marketing campaigns for critically acclaimed video games, including "Halo 3". While at NBC Universal, he oversaw the successful launch of the all-new www.biggestloser.com website. Jeff has served as an advisor to digital marketing agencies Organic, Inc. and MXM in the automotive, consumer electronics, entertainment, and travel industries. He spent 12 years at Ford Motor Company, including serving as Managing Director of Ford Spain and five years at Chrysler as Vice President and General Manager of Chrysler and Jeep Divisions. Jeff graduated from Kenyon College Magna Cum Laude; he was a member of Phi Beta Kappa and an Academic All-American in football. He holds master's degrees from Johns Hopkins University and Wharton School of the University of Pennsylvania.

**Kathy Pinson, Chief Operations Officer** – Since starting with the Company in 1979, Ms. Pinson has served with distinction in a number of roles, including Manager of Accounting and Regulatory Compliance, Vice President (1982), and Controller (1989). A Certified Public Accountant, she served on the Company's Board of Directors from 1990-2002 and currently serves on the Corporate Marketing Team.

### III. DESCRIPTION OF LEGALSHIELD'S LEGAL AND IDENTITY THEFT SERVICES SYSTEM (continued)

**Steve Williamson, Chief Financial Officer** – Steve Williamson has been with LegalShield for over 15 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.

**Jack Goldenberg, Executive Vice President and Chief Technology Officer** – Joined LegalShield in January 2015 to establish and lead the company's technical vision and development, including strategy for technology platforms and partnership. In his previous career, he served Meredith Corporation as Senior Vice President and Chief Technology Officer for the National Media Group. In this role, Jack managed delivery of Meredith Digital Tablet editions for all of the Meredith magazine brands, including interactive editions for Better Homes and Gardens, Parents, Fitness, and family Fun. Prior to Meredith, Jack served as Chief Technology Officer for Enterprise Media Group at Dow Jones and Company. He was responsible for delivering the innovative Dow Jones Investment Banker and Dow Jones Adviser digital products. His background also includes serving as the Senior Vice President, Content Technology for Thomson Reuters/Thomson Financial. Under his leadership, Thomson Reuters was able to implement new technology to streamline the data acquisition and delivery process, resulting in faster and more reliable delivery to the customer. Mr. Goldenberg hold a bachelor's degree in professional science from C. W. Post University. He also served as a board member for the Des Moines Playhouse. A nonprofit organization, from 2011 through 2014.

#### **Data**

All information is stored on LegalShield servers located in the United States. Procedural and technical safeguards are in place to protect personal information against loss or theft as well as unauthorized access and disclosure. Information is treated as an asset that must be protected against loss and unauthorized access. Several 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 our website. Each associate and member have a unique user name and password that must be entered every time a user logs on to our 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 our web site or calls to customer service representatives
- Information about your transactions with LegalShield, our affiliates or others.

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

### **III. DESCRIPTION OF LEGALSHIELD'S LEGAL AND IDENTITY THEFT SERVICES SYSTEM** *(continued)*

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

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

#### **Boundaries of the 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.

#### **Procedures**

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

- Setup new member accounts based on the type of plan purchased;
- Setup secure data transfer for group accounts; and
- Setup 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; and
- 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.