Structures Inc.

A Subsidiary Company of Integrated Financial Systems, Inc.

System and Organization Controls (SOC) 3 Report

Structures Inc.'s Description of its Structured Settlements Services System

For Security Trust Service Criteria

For the Period December 1, 2020 to October 31, 2021

Young & Associates
Certified Public Accountants

INDEPENDENT SERVICE AUDITOR'S REPORT

To: The Management of Structures Inc.

Scope

We have examined management's assertion, contained within the accompanying "Management's Report on its Assertion on the Effectiveness of Controls Over its Structured Settlements Services System based on the Trust Services Criteria for Security" (Assertion), that Structures Inc.'s ("Structures") controls over the Structured Settlements Services System (System) were effective throughout the period December 1, 2020 to October 31, 2021, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the trust services criteria relevant to security (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

Structures 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 Structured Settlements 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; and,
- Identifying, designing, implementing, operating, and monitoring effective controls over the Structured Settlements Services 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 (1) obtaining an understanding of Structures' relevant security polices, processes and controls, (2) obtaining an understanding of the principal service commitments and system requirements, (3) assessing the risks that controls were not effective to achieve Structures' principal service commitments and system requirements, (4) testing and evaluation of the operating effectiveness of the controls, and (5) 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 obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Young & Associates
Certified Public Accountants

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, any projection of the evaluations of effectiveness to future periods, or conclusions about the suitability of the design on the controls to achieve Structures' principal service commitments and system requirements, is subject to the risk that the controls may become inadequate because of changes in conditions, that the degree of the 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, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal controls at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, Structures' controls over the system were effective throughout the period December 1, 2020 to October 31, 2021, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

Young & Associates, LLP

November 23, 2021

Management's Report on its Assertion on the Effectiveness of Controls Over its Structured Settlements Services System based on the Trust Services Criteria for Security

We, as management of, Structures Inc. are responsible for:

- Identifying the Structured Settlements Services System ("System") and describing the boundaries of the system, which are presented in Attachment A;
- Identifying the principal service commitments and system requirements that are the objectives of our system, which are presented in Attachment B;
- Identifying the risks that would threaten the achievement of our principal service commitments and service requirements;
- Identifying, designing, implementing, operating, and monitoring effective controls over the 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.

We assert that the controls over the system were effective throughout the period December 1, 2020 to October 31, 2021, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security set forth in *TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

Very Truly yours,

The Management of Structures Inc.

Attachment A- Structures Inc.'s System

Components of the System

Infrastructure

Structures' information systems consist of facilities, computers, mobile devices, storage systems, and networking communication equipment both in a corporate infrastructure and a cloud environment infrastructure. Additionally, hosted e-mail, security, content, and collaboration services are in use. The Structures infrastructure supports internal users for shared functions such as application development and quality assurance teams to develop and qualify software releases. Database, application hosting, application delivery services, and multiple monitoring services are hosted on this infrastructure. This corporate infrastructure is distributed between the Structures corporate headquarters in Atlanta, Georgia and the IFS corporate headquarters in Greenwood Village, Colorado and the Databank co-location facility in Englewood, Colorado. All relevant data is backed up using encryption and off-site data transfer procedures. These systems are operated under the strategic guidance of the Vice President of Information Technology and Security.

Software

The System is used to store and process information related to the settlement of insurance claims as well as information related to the purchase of annuities and other services on behalf of the claimant. This information is acquired from, and in some cases shared with, claims organizations ("Case Originators"), attorneys, life insurance companies, and other service providers. Specifically, Structures utilizes its Salesforce System, along with the supporting computing and communications infrastructure.

People

Structures Management

Structures Management, which consists of the managers and department heads, is responsible for overall security, ensuring enforcement of controls, approving risk assessment, selection, and prioritization of risks to mitigate, and to provide oversight of the Structures control environment.

Structures Management has made a commitment to discovering and addressing any security shortcomings and has supported its commitment by devoting resources to these efforts. This ethical attitude of critical self-assessment supports an organizational environment in which Structures can meet those commitments and satisfy customer and regulatory expectations.

Procedures

Structures has operational procedures in place to help ensure that security commitments can be met. Standard security commitments include, but are not limited to, the following:

- Identifying and documenting the security needs of authorized users;
- Assessing risks on a periodic basis;
- Preventing unauthorized access;
- Adding new users, modifying the access levels of existing users, and removing users who no longer need access;
- Assigning responsibility and accountability for system security;
- Assigning responsibility and accountability for system changes and maintenance;
- Testing, evaluating, and authorizing system components before implementation;
- Addressing how complaints and requests relating to system security issues are resolved;
- Identifying and mitigating security breaches and other incidents;
- Providing training and other resources to support the system security policies;
- Providing for the handling of exceptions and situations not specifically addressed in its system related security policies;
- Providing for the identification of consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements; and,
- Sharing information with third-parties.

Regularly reviews security metrics to ensure that these commitments are met. In the event material changes are made that decrease the level of security commitments, Structures will notify system users via the Structures website, e-mail, or other means.

Structures has put into place a set of policies and procedures documented within the Information Security and Privacy Policy ("Information Security Policies") to help ensure that security commitments can be met. The Structures Information Security Policies consist of a set of policies and procedures that define how internal data, systems, and resources are secured and protected from unauthorized access, attempted intrusions, and service disruptions. Along with standard operating procedures, Structures Management has identified and implemented control procedures to enhance Structures' security posture.

Data

Data includes printed and electronic data or information submitted by its clients, life company partners, as well as attorneys and other parties related to the matters in which Structures is involved. This data includes prospective annuitants' medical history, personally identifiable information, and other sensitive information used to provide the Company's structured settlement services. This information is provided to users of the System in several ways: voice conversation on the phone or in person interview, or electronic communications. Access to information is restricted to authorized personnel and access is granted after receiving proper approval from Structures Management.

Boundary of the System

Structures works with insurance companies, attorneys, and injured parties to securely present annuity payment information from its Salesforce application to meet the needs of its customers through its Structured Settlements System.

The System includes the infrastructure, software, people, procedures, and data required to deliver the Structured Settlements System to its customers and meet Structures' security commitments.

Attachment B- Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by Structures Management to customers regarding the performance of Structures' system. Structures communicates its commitments via contracts. Structures' service commitments and system requirements include a secure environment for the data stored and processed by the system. Structures' commitments include the following:

- Manage the assessment and treatments of risks and continually improve its information security posture.
- Protect the physical assets that contain customer data.
- Ensure systems containing customer data are used only by approved, authenticated users.
- Ensure personnel entitled to use systems gain access only to the customer data that they are authorized to access.
- Ensure data remains secure throughout processing and remains intact after processing activities.
- Ensure data is protected from accidental destruction or loss, and the timely access, and restoration of data in the event of a service incident, that is managed according to contractual agreements with its customers.
- In the event of a security breach of data, the effect of the breach is minimized, and the customer is promptly informed.
- Ensure Structures regularly tests, assesses, and evaluates the effectiveness of the technical and organizational measures.
- Maintain appropriate administrative, technical, and physical security measures to protect data against unauthorized access, disclosure, and loss. Structures will host all customer data in the United States.
- Comply with the applicable regulations including the New York Department of Financial Services (NYDFS).
- Manage customer data according to its Information Security and Privacy Policy and its contractual agreements with its customers.

System requirements are specifications regarding how Structures should function to meet the Company's commitments to customers. Requirements are specified in the Company's policies and procedures, which are available to all internal users of the system. The Company's system requirements include the following:

- Logical access standards
- Physical access standards
- Employee provisioning and deprovisioning standards
- Access reviews
- Encryption standards
- Intrusion detection and prevention standards
- Risk and vulnerability management standards
- Configuration management
- Incident handling standards
- Change management standards
- Vendor management