I.C. SYSTEM, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS COLLECTION PROCESSING SYSTEM

System and Organization Controls 3 (SOC 3^{SM}) Report

With Independent Service Auditor's Report Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy throughout the Period December 1, 2022 to November 30, 2023

INDEPENDENT SERVICE AUDITOR'S REPORT

Members of the Board and Management
I.C. SYSTEM, INC.

Scope
We have examined I.C. System, Inc.'s (I.C. System) accompanying assertion titled "Assertion of I.C. System, Inc.'s Management" (assertion), that the controls over its collections processing system were effective throughout the period December 1, 2022 to November 30, 2023, to provide reasonable assurance that I.C. System's service commitments and system requirements were achieved based on the criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria) set forth in the AICPA's TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

Service Organization's Responsibilities
I.C. System 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 I.C. System's service commitments and system requirements were achieved. I.C. System has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, I.C. System is responsible for selecting, and identifying in its assertion, the applicable trust service 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 whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination 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 I.C. System'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 I.C. System'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 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 I.C. System's collection processing system were effective throughout the period December 1, 2022 to November 30, 2023, to provide reasonable assurance that I.C. System's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Respectfully submitted,

LB Carlson, LLP

LB CARLSON, LLP
Minneapolis, Minnesota

January 5, 2024

ASSERTION OF I.C. SYSTEM, INC.'S MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within I.C. System, Inc.'s collection processing system throughout the period December 1, 2022 to November 30, 2023, to provide reasonable assurance that I.C. System's service commitments and system requirements relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 1, 2022 to November 30, 2023, to provide reasonable assurance that I.C. System's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy* (AICPA, *Trust Services Criteria*). I.C. System'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 systems were effective throughout the period December 1, 2022 to November 30, 2023, to provide reasonable assurance that I.C. System's service commitments and system requirements were achieved based on the applicable trust services criteria.

Tom Emms
Chief Information Officer
I.C. System, Inc.

January 5, 2024

ATTACHMENT A – I.C. SYSTEM, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS COLLECTION PROCESSING SYSTEM

Company Overview

Services Provided

I.C. System provides accounts receivable management services in the following industry-specific units:

- Financial Services
- Telecommunications
- Utility
- Retail
- Medical/Healthcare
- Government

The business units rely on a centrally located and managed information technology (IT) infrastructure and standard corporate functions that are located at the corporate headquarters in St. Paul, Minnesota.

I.C. System offers a variety of contract options and relationships with its customers, along with a variety of services, including:

- Early-out Collections.
- Inbound and Outbound Customer Service Calls.
- Skip Tracing.
- Late-Stage Delinquency Collections.
- Charge-Off Collections.

Background

I.C. System is a privately owned provider of accounts receivable management services headquartered in St. Paul, Minnesota and services over 6,000 clients across several major industry sectors. Founded in 1938, I.C. System focuses on achieving a high standard through the ethical treatment of consumers, clients, and employees. For over 80 years, I.C. System's goal has been to conduct business with integrity and consumer-friendly practices.

To achieve its ethical goals, I.C. System seeks to improve the debt collection experience for its clients and their consumers. The niche of being "the best, most trusted provider of receivable management services" underlines I.C. System's strong foundation in ethics. Above all, I.C. System's Core Values influence every aspect of the organization, from creating a positive consumer experience to training employees to conduct themselves in a consumer-friendly fashion. Core Values include:

- PEOPLE: We treat people with dignity and respect.
- INTEGRITY: We do the right thing.
- PERFORMANCE: We deliver results that exceed expectations.
- PRIDE: We are proud of what we do and how we do it.
- INNOVATION: We find better ways to get things done.

I.C. System's devotion to its Core Values has resonated with its employees and earned recognition throughout the community. _The Star Tribune_ has named I.C. System a Top Workplace each year from 2017-2023.

Additionally, I.C. System's ethical approach to past-due account recovery has been given an "A" rating by the Better Business Bureau (BBB). I.C. System also is a four-time finalist for BBB's Torch Award for Ethics.

I.C. System uses an application system for collecting debts owed to their clients. The application system is an internally developed and internally maintained software package that operates on an Intel-based Dell server. I.C. System uses letters (mail, email, or text), phone calls, or a combination of both as primary means to collect debt.

Entity-level controls at I.C. System are in place to establish senior management's "Tone at the Top" for the organization. These controls form the basis and environment by which the controls operate and reflect senior management's attitude, awareness, and actions concerning the importance of internal control. The controls also demonstrate the emphasis placed on control in the policies, procedures, methods, and organizational structure of I.C. System.

Components of the System Used to Provide the Services

Infrastructure

I.C. System's production domain includes Web servers, database servers, file servers, Secure File Transfer Protocol (SFTP) servers, virtual servers, encrypted storage area network (SAN). Firewalls include a demilitarized zone (DMZ) to protect the internal network from external access over the Internet as well as IPS. I.C. System's headquarters securely houses these systems. Management of firewalls occurs in-house, whereas I.C. System outsources the management of the intrusion detection system (IDS) to a subservice organization.

Software

The primary system used for collections is physically located at its headquarters and is developed and maintained in-house.

People

The oversight for collections processing provided by I.C. System is assigned to the President/Chief Executive Officer and Chief Financial Officer (CFO). Other key individuals responsible for collections processing are the Senior Vice President (SVP) Collections Operations, Compliance Officer, and Chief Information Officer (CIO).

Key work groups include:
- **_Management_**
  Management is involved, on an ongoing basis, in operational decisions and issues that affect the business. Management meets regularly to review and approve strategic planning and policies, and monitor I.C. System's daily activity. Management plans and budgets on an annual basis. Business review meetings occur monthly, with attendance of VP-level staff and above. Management

discusses department updates and issues. The Executive Management Team meets regularly and as needed.

- *Human Resources*
  The Human Resources (HR) department is responsible for employee recruitment and hiring practices, employee orientation, maintaining performance evaluations, benefits, and facility access controls.
- *Client Services*
  Client Services staff are available from 7:00 AM to 6:00 PM CST. Clients are able to contact I.C. System via email, online tools, phone, U.S. mail, daily files, or facsimile. Clients also may contact I.C. System via an 800-telephone number that tracks incoming calls. Most incoming calls relate to the posting of payments, closing of accounts, account disputes, etc. Client Service Representatives enter the client information into the application system.
- *Security Team*
  Led by the CIO, the Security Team is responsible for implementation and oversight of data and physical security.

Procedures and Processes

Written policies and/or procedures have been designed to include a mixture of automated and manual procedures, broadly categorized in the following areas:

- Information security policies.
- HR policies.
- Computer operations manual.
- Business continuity/disaster recovery plan.
- System specifications, requirements, and updates.
- Training documentation.

The processes designed by I.C. System to achieve the organization's service commitments and system requirements follow policies and procedures outlined above, consisting of manual and automated (system-generated) processes throughout the collections processing cycle. This section outlines the processes utilized by the organization to provide the collections processing services.

File Entry Process

The process to enter files into the application system includes the following steps:

- I.C. System receives an encrypted file from a client through a managed file transfer product.
- Use of SFTP whenever possible and includes a PGP-encrypted file.
- The managed file transfer product decrypts the file and puts the data into a client specific network-processing folder.
- ETL software takes the file and reformats the data as needed.
- Files created during the day are processed and loaded into the collection application system at 4:00 PM CST on business days.
- Processing of files occurs nightly to ensure availability to collectors in the morning. During the processing, the system performs address and phone scrubs to verify the file.
- The final step is encrypting the new client file in the processing folder and moving it to the backup directory for long-term storage, and also removing it from the processing folder.

Collection Services

The collections services covered by this system description include:

- *Early-Out Collections*

  At I.C. System, early-out collections in healthcare (HC) means first-party collections or collections in which the call is made as an extension of the HC system's own collections department. The I.C. System representative answers calls with the name of the HC system and not as I.C. System. In HC, the task is still collections, but I.C. System may charge a contingency fee and an additional flat fee to research insurance claims.

  In other industries, early out is synonymous with pre-collect or pre-charge-off. In these cases, the debts are very early stage third party, and I.C. System answers a call by identifying themselves as I.C. System. The term simply refers to the fact that the debt is in the early stage of delinquency (four to 30 days past due), and in most cases, has not been charged off.

- *Inbound and Outbound Customer Service Calls*

  For some clients, I.C. System is acting as an extension of, or is replacing, the client's in-house call center. Therefore, like HC's early out, I.C. System answers or places calls in the name of the client. Also in these situations, I.C. System frequently does not charge a contingency fee, but rather charges a "per minute" rate for a call or a daily full-time equivalent (FTE) rate for the person on the phones.

- *Skip Tracing*

  Skip tracing is the term applied to the task of attempting to locate a consumer who has moved, disconnected their phone, or in some other way made it difficult to be located. Skip tracing is conducted using a number of subscription services that maintain databases of information about people.

- *Late-Stage Delinquency Collections*

  This term usually refers to debts that have been uncollectable through the first few stages of debt collection and now are "late stage". These debts could be candidates for placement into a warehouse or "trigger" program.

  A debt, if uncollected, usually goes through many phases of collection. Initially, debt received by a third-party collection agency either is referred to as "pre-collect" (if not charged off) or "primes"/ "primary" (if already charged off). At any point, the client may pull the debt from the primary agency and place it with a "second" or "secondary" agency for further attempts to collect. After another prescribed period, the client may pull it again and place the debt with a third or "tertiary" agency. Some clients will even place debts with a fourth or "quad" agency.

  Depending on the client and their overall collection strategy, late stage could occur any time after it has been in the "Second Stage" (if it will be left in the second stage indefinitely), up to and including a quad placement.

- *Charge-off Collections*
  Clients make the determination to write off, or charge off, a debt. At the time of write off, they are typically looking to recoup any amount, with the understanding that it will likely be minimal in comparison to the original amount. The clients turn over the debt to a debt collection agency, who attempt to collect the debt; and then charges a contingency fee if successful.

Data

Data processed by the collections processing system consists of data subjects ("consumer") names, addresses, social security numbers, phone numbers, dates of birth, and potentially other personal identified information as required to perform the collection services.

Most collections occur either via letter (mail, email, and text) or phone call to the consumer, with a combination of both methods typically used to collect payments. The method used is dependent upon the client's requirements. Documented procedures exist for the input of transactions.

Clients send data to I.C. System via U.S. mail or secured FTP, with the files typically being encrypted using PGP. Upon initial receipt of electronic client files, there is a cursory review (to verify the file is not corrupt) prior to beginning the processing of that file. After reviewing, the data files are loaded into the system. The data center, which is part of IT operations, loads this data and processes the data files. Control over the receipt of input files verifies the data maintains integrity, and that input is from authorized users. Control strings verify processing of records in the proper sequence.

On a daily basis, I.C. System sends a data file (via encrypted method) to a vendor for standardization of addresses and phone numbers. The vendor returns the data file (via encrypted means) and I.C. System processes the data. Generation of a file occurs during a nightly batch process for a subservice organization to create letters for data subjects. This subservice organization creates and mails the letters (mail or email) to data subjects on behalf of I.C. System.

Payments and Fees

Completion of payment processing and fee determination occurs via batch processes on the systems as follows:

- Payment batch processes post to the system throughout the day. Nightly, a validation process runs to assess fees and post the funds to the client's account, as well as the I.C. System receivables. The billing process is cycle driven.
- Daily, weekly, and monthly reconciliation activities occur, and the investigation and resolve process for errors take place on a daily basis. Daily generation and review of reports verify proper processing of the previous night's batch files.
- Bankruptcies have various codes based on the type and chapter of the bankruptcy files. Collection efforts cease upon I.C. System's receipt of proof for the bankruptcy. If the consumer has not provided the information, I.C. System generates a letter requesting the information. Until the consumer provides information about the bankruptcy, I.C. System delays collection efforts. Upon receipt of bankruptcy proof, I.C. System sends a special action notice to the client to notify them of the bankruptcy.

- Due to both regulatory requirements and client requirements, consumer status tracking occurs in the system to ensure no consumer receives calls more frequently than allowed. Nightly runs of a batch process create the work queues used by collectors the following day. If there are errors in the file loading, IT operations investigates and resolves the errors in a timely manner. I.C. System assumes the file remained intact and correct in the event of no errors in the loading process.
- There are confidentiality and availability clauses included in vendor contracts as part of the normal contract process.
- Credit Bureau Dispute:
    - Client contracts define which organization has credit bureau reporting responsibility. Most I.C. System clients choose to have I.C. System handle this function.
    - A consumer first pulls their credit report from one of the three bureaus: Experian, TransUnion, or Equifax. When a consumer sees a collection trade line posting from I.C. System, they dispute the accuracy directly with I.C. System and/or notify the bureaus and fill out an Automated Consumer Dispute Verification (ACDV) Form. The bureau uses a company called E-OSCAR to send the ACDV Form to I.C. System for investigation. I.C. System then verifies the details surrounding the debt with their own internal systems and then resubmits the updated information through E-OSCAR to make the changes and/or corrections if necessary. There is a regulatory requirement to answer disputes within 30 days of the bureau receiving them.
    - If the consumer is still showing in the system as owing the money, the consumer calls I.C. System to have the debt investigated further. This involves providing proof of payment information. The client that originally submitted the debt for collections uses this information to verify the status of the debt. I.C. System updates the status with the bureaus based on results of the investigation. If the debt information is not valid, I.C. System requests the national credit reporting agencies to delete the trade line from the consumer's credit record.
- Billing Process:
    - Billing occurs in accordance with contract terms. Terms are typically based on a contingency fee, a unitary fee, or a combination of both. Upon signing a contract, the client services sales support staff enter the contract details into the system used by the group working for a specific client. I.C. System collects these payments, or the customer may receive payments and notify I.C. System of the payment.
    - I.C. System staff receive payments either electronically or via U.S. mail. When received via U.S. mail, payment information is entered into a payment remittance processing system. This system creates a file to upload nightly to post to the appropriate accounts.
    - I.C. System makes payments to clients at least monthly, though different clients may have different cycles of payment. I.C. System bases payment dates primarily on the state in which the client is located and makes payments via a hard-copy check mailed to the client's location.
    - In the event of the return of a consumer's payment for nonsufficient funds (NSF) or for other similar reasons, I.C. System reverses the credits against the debt and the collection effort begins again. Return of the consumer's payment net against the client's next payment through a reduction of the check by the returned amount.

ATTACHMENT B – PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Principal Service Commitments and System Requirements

I.C. System designs its processes and procedures to meet its objectives for its collections services. Objectives are based on service commitments made to user entities and the financial, operational, and compliance requirements established for the services. The collections services are subject to the requirements of the Fair Debt Collection Practices Act (FDCPA), including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which I.C. System operates.

Documentation and communication of commitments occurs through Service Level Agreements, customer agreements, and on the customer-facing website. Baseline security commitments are standardized and include, but are not limited to, the following:

- Compliance with various frameworks including, but not limited to, the following:
  - PCI DSS v4.0 Annual Certification which validates secure processing, storing and transmitting all consumer data.
  - HIPAA and HITECH security provisions, safeguarding rules, and confidentiality concerns regarding the transmission, use, and storage of healthcare information.
  - Financial Services Modernization Act of 1996 for the certification to collect and store consumer data with security and confidentiality. To be compliant means that I.C. System:
    - Ensures the security and confidentiality of customer records and information.
    - Protects against any unanticipated threats or hazards to the security or integrity of such records.
    - Protects against unauthorized access to or use of such records or information.
- Encryption technologies utilized to protect data at rest and in transit.
- Physical and logical controls implemented to limit access based on the concept of least privilege.
- Quarterly internal and external vulnerability scans and annual penetration testing performed by third parties.
- Two-factor authentication required for remote access to the system.
- Mandatory annual security training for all employees.
- Use of the following password complexities:
  - Passwords contain a minimum of 12 characters, including three of the four following categories of characters:
    - Uppercase letters
    - Lowercase letters
    - Numbers
    - Special characters
  - Passwords expire every 90 days.
  - Users cannot re-use the last 24 passwords.
  - Minimum two day lifetime passwords.

I.C. System establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Communication of system requirements occurs through I.C. System's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to the protection of systems and data. These include policies around the design and development of the service, system operations, management of the internal network, and the hiring and training of employees. In addition to these policies, documentation of standard operating procedures on how to carry out specific manual and automated processes required in the operation and development of collections services are available.