Credit Control Corporation

Financial Receivables Specialists

Service Organization Control (SOC) Report – SOC 1, Type 2

Report on a Description of Credit Control's System for Providing Account Management and Collection Services, and the Suitability of the Design and Operating Effectiveness of Controls

For the period June 1, 2018 to May 31, 2019

Table of Contents

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT PROVIDED BY PBMARES, LLP

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Credit Control Corporation
Newport News, Virginia

Scope

We have examined the attached description entitled, "Credit Control Corporation's Description of Its System for Providing Account Management and Collection Services" for processing user entities' transactions throughout the period June 1, 2018, to May 31, 2019, (the "description") and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Credit Control Corporation's Assertion" (the "assertion"). The controls and control objectives included in the description are those that management of Credit Control Corporation believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Account Management and Collection Services system that are not likely to be relevant to user entities' internal control over financial reporting.

The information included in Section V, "Other Information Provided by Credit Control Corporation (Unaudited)," is presented by management of Credit Control Corporation to provide additional information and is not a part of Credit Control Corporation's description of its Account Management and Collection Services system made available to user entities during the period June 1, 2018, to May 31, 2019. Information about Credit Control Corporation's "Management's Response to Results of Tests Performed" has not been subjected to the procedures applied in the examination of the description of the Account Management and Collection Services system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the Account Management and Collection Services system, and accordingly we express no opinion on it.

Credit Control Corporation uses various subservice organizations in delivering its' Account Management and Collection Services system. The description includes only the control objectives and related control objectives of Credit Control Corporation and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by Credit Control Corporation can be achieved only if complementary subservice organization controls assumed in the design of Credit Control Corporation's controls are suitably designed and operating effectively, along with the related controls at Credit Control Corporation. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitably of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Credit Control Corporation'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.

Service Organization's Responsibilities

In Section II of this report, Credit Control Corporation has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Credit Control Corporation is responsible for preparing the description and assertion, including the completeness, accuracy and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, 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 the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period June 1, 2018, to May 31, 2019. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the controls includes:

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- Evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not; therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing and results of those tests are listed in Section IV of this report.

Opinion

In our opinion, in all material respects, based on the criteria described in Credit Control Corporation's assertion:

- The description fairly presents the Account Management and Collection Services system that was designed and implemented throughout the period June 1, 2018, to May 31, 2019.
- The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period June 1, 2018, to May 31, 2019, and subservice organizations and user entities applied the complementary controls assumed in the design of Credit Control Corporation's controls throughout the period June 1, 2018, to May 31, 2019.
- The controls operate effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period June 1, 2018, to May 31, 2019, if complementary subservice organization and user-entity controls assumed in the design of Credit Control Corporation's controls operated effectively throughout the period June 1, 2018, to May 31, 2019.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV of this report, is intended solely for the information and use of management of Credit Control Corporation, user entities of Credit Control Corporation's Account Management and Collection Services system during some or all of the period June 1, 2018, to May 31, 2019, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

PBMares, LLP

Norfolk, Virginia
July 10, 2019

SECTION II

CREDIT CONTROL CORPORATION'S MANAGEMENT ASSERTION

Credit Control Corporation
Financial Receivables Specialists

Credit Control Corporation's Assertion

We have prepared the description of Credit Control Corporation's Account Management and Collection Services system entitled, "Credit Control Corporation's Description of Credit Control's System for Providing Account Management and Collection Services", for processing user entities' transactions throughout the period June 1, 2018, to May 31, 2019 (the description) for user entities of the system during some or all of the period June 1, 2018, to May 31, 2019, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

Credit Control Corporation uses various subservice organizations in delivering its' Account Management and Collection Services. The description includes only the control objectives and related controls of Credit Control Corporation and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organization.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Credit Control Corporation's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

- The description fairly presents the Account Management and Collection Services system made available to user entities of the system during some or all of the period June 1, 2018, to May 31, 2019, for processing their transactions. The criteria we used in making this assertion were that the description:
    - Presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including, as applicable:
        - The types of services provided, including, as appropriate, the classes of transactions processed
        - The procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary and transferred to the reports presented to user entities of the system
        - The information used in the performance of procedures including, as applicable, related accounting records, whether electronic or manual, and, supporting information involved in initiating, authorizing, recording, processing and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information presented for user entities

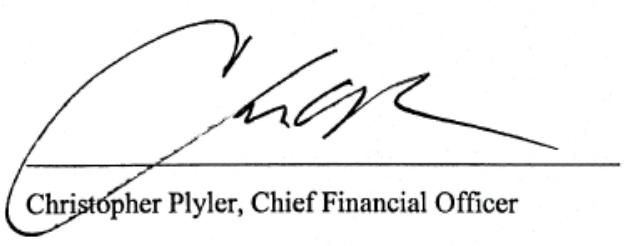
- How the system captures and addresses significant events and conditions, other than transactions
- The process used to prepare reports and other information for user entities
- Services performed by a subservice organization, if any, including whether the carve-out method or inclusive method has been used in relation to them
- The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls
- Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities and monitoring activities that are relevant to the services provided

  - Includes relevant details of changes to the service organization's system during the period covered by the description
  - Does not omit or distort information relevant to the scope of the service organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the Account Management and Collection Services system that each individual user entity of the system and its auditor may consider important in its own particular environment

- The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period June 1, 2018, to May 31, 2019, to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of Credit Control Corporation's controls throughout the period June 1, 2018, to May 31, 2019. The criteria we used in making this assertion were that:

  - The risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.
  - The controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.
  - The controls were consistently applied as designed; including whether manual controls were applied by individuals who have the appropriate competence and authority.

Credit Control Corporation



Christopher Plyler, Chief Financial Officer

SECTION III

CREDIT CONTROL CORPORATION'S DESCRIPTION OF ITS SYSTEM FOR PROVIDING ACCOUNT MANAGEMENT AND COLLECTION SERVICES THROUGHOUT THE PERIOD JUNE 1, 2018, TO MAY 31, 2019

Company Overview

R & B Corporation of Virginia d/b/a Credit Control Corporation (Credit Control) serves as an outsource vendor providing accounts receivable management and support services primarily to healthcare providers and tele-communications companies throughout the United States. Located in Newport News, Virginia, the objective of Credit Control is to provide effective collection service by delivering account recoveries with minimal consumer complaints.

Overview of Account Management and Collection Services

Credit Control currently offers an expanded menu of Account Management and Collection Services under each division.

Bad Debt Recoveries

- Collect outstanding balances on delinquent accounts for healthcare and telecommunication clients
- Contact debtors via inbound/outbound phone calls, Fair Debt Collection Practices Act (FDCPA) compliant letters and other means of communication
- Skip trace accounts to locate customers and maintain current contact information
- Send past-due notices for delinquent accounts and/or missed settlement payments
- Report proper balances to credit bureaus in accordance with Fair Credit Reporting Act (FCRA)
- Investigate and resolve complaints and/or disputes regarding debt collection attempts
- Ensure customer privacy in accordance with applicable guidelines
- Forward accounts to attorney for litigation when requested by client

Pre-Collection Services

- Collect outstanding balances on accounts which are not yet delinquent
- Remote staffing for extended business office support
- Follow-up of unpaid third-party insurance claims
- Establish payment plans in accordance with client guidelines
- Legacy system accounts receivable management
- Custom programs to meet specific client goals/objectives

Key Components of the System

Infrastructure

Data security is multi-tiered and comprised of firewalls at the network boundary, and incorporates Symantec Endpoint Protection at the desktop level which employs virus, email, spyware, network, web, and proactive threat protection. Third party email scanning is also utilized to provide an additional layer of security. Credit Control employs both Cisco and Juniper devices in order to securely connect to client systems.

Outbound telephone campaigns are accomplished via IAT SmartDial predictive dialer solution. In May 2019, Credit Control migrated to RingCentral's InContact call center and office phone system solution. With a secure, reliable, and flexible VOIP platform, Credit Control is able to manage all business communications from desktop, laptop or mobile device in any location. High quality calls in HD voice, audio conferencing, online fax, and SMS are advantageous for the overall collection effort. RC's automated dialer performs selectively in three different modalities: predictive, preview, and agentless. Dialer campaigns are designed to maximize the effectiveness of outbound call routines. All calls are digitally recorded for quality assurance purposes. It facilitates predictive, preview, and agentless modalities and is

capable of initiating thousands of contact attempts per day. Individual collector productivity is managed via a communications server running call-tracking software, which can measure all outgoing calls, call duration, and other call related statistics. All incoming and outgoing calls are recorded for quality and training purposes via a digital call recording application.

Credit Control's website, www.credcontrol.com is supported internally by the IT Department. It offers the "Client Access" interactive feature for clients wishing to view their accounts in the same manner as our staff does. Website development is an evolving process whereby its capabilities are continuously enhanced in support of improved agency/client/consumer relationships, needs, and security requirements.

Software

Credit Control utilizes an Intelec/RMEx "smart collection" software system to manage all collection processes and client/consumer data and activities. A key feature is its seamless integration with dialer management. The system was developed and is supported by the Quantrax Corporation.

- Standard system reports provided include:
    - Activity History (recovery results)
    - Placement History (placement analysis)
    - Status Report (account level detail)
    - Weekly/Month-end Client Statements
    - Acknowledgement (reconciliation)
    - Close-out with Reason and Close Code
- Frequency of reports are available upon demand or scheduled on a daily/weekly/monthly basis according to client needs.
- Availability of ad hoc reports through the IBM Query option and custom programming designed by our IT Department.
- Custom financial reporting via a multitude of products integrated with Intelec/RMEx.
- Transparency to real time activity is available through the Credit Control website at www.credcontrol.com using the "Client Access" feature. Clients can view all account activity, comments, notes, etc. in Intelec/RMEx as seen by Credit Control staff.

Payment Vision – provides a PCI-certified electronic payment services gateway that connects to the ACH and credit card network, which allows Credit Control to securely accept electronic payments via phone, web or interactive voice response (IVR).

Interactive Data – provides a Cell Suppression product that proactively enables Credit Control to identify and suppress cell phone numbers from its caller lists. A high degree of accuracy is required to remove any doubt around compliance-related dialling issues. Interactive Data also provides a bankruptcy scrub for all new business accounts. It is updated daily with the data derived from the US courts systems.

Overview of Account Management and Collection Services Procedures

A. Standard Collection Process Schematic:

Step	Description	Responsible Party
1	*Placement File received by Client via FTP server for upload into Intelec RMEx*	*Client*
2	Accounts scrubbed for addresses, duplicates, cell phones, deceased and bankruptcy	Agency
3	Case number assigned	Agency
4	Account assigned to specific Master Client Number (125XXX)	Agency
5	Acknowledgement Report sent to Client	Agency
6	*Account withdrawals requested as soon as possible*	*Client*
7	Written Letters/Notices: - FDCPA Compliant First Notice sent on 2nd day following placement - NCOA48 scrub for most current address - Additional notices/letters sent based on debtor response - Credit reporting (TransUnion, Equifax, Experian) if not paid within 45 to 90 days	Agency
8	After 5 days and no payment, account appears on collector work maps	Agency
9	Phone calls begin on 5th day - Calls continue every 6 working days for 60 days - Unpaid account balance is credit reported on day 61 - Calls continue every 10 working days for days 61-90 - After 90 days, additional call campaigns generated as necessary	Agency
10	Customer Payments are received by Agency via: - Mail - Checks/Money Orders/Bankcard - Phone (Live Agent) – Bankcard (MasterCard/Visa/Discover) - Phone (IVR) – Bankcard or Check (using check routing number) - Online – Payment Vision	Agency
11	Payment Plans established consistent with Client guidelines	Agency

Step	Description	Responsible Party
12	*Payments received by Client reported when received by FTP or mail*	*Client*
13	Funds Wired to Client Daily, Weekly or Monthly	Agency
14	Monthly Reports sent to Client - Placement History Report - Activity History Report - Close-Out Report - Monthly Statements (Invoices)	Agency

Regulatory Requirements and Compliance

Consumer Financial Protection Bureau (CFPB) – The CFPB is an independent, self-governing federal agency within the Federal Reserve System, which serves to protect consumers from potentially abusive/harmful financial practices. Third party debt collectors such as Credit Control are subject to its enforcement actions and policies. The bureau often works in concert with state Consumer Protection Agencies/Attorneys General Offices. The CFPB was created under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act).

- Credit Control Corporation (Credit Control) is a registered stakeholder with the CFPB.
- The CFPB notifies Credit Control via email when a consumer files a complaint about an account on-file.
- Credit Control then accesses the CFPB portal to view and copy the consumer's complaint.
- Credit Control maintains an Excel log in order to document complaints by the date received.
- Each complaint is managed by the Compliance Officer who researches the consumer's issues and utilizes staff resources within the Medical and Cable Collection and Clerical Divisions to investigate accounts and/or to access data from original creditors.
- Once an investigation is completed, the Compliance Officer responds to the consumer via the CFPB portal; advising them of details pertinent to the account(s) in question and answering questions/concerns expressed by the consumer.
- The CFPB portal retains an electronic copy of each complaint/response in an Archive file.
- Credit Control retains a paper copy of each complaint/response by date in a file located in the Compliance Officer's office.

Health Insurance Portability and Accountability Act (HIPAA) – HIPAA legislation was enacted by Congress to ensure the "portability" of health insurance coverage and to mandate standards for the exchange of "protected health information" (PHI). These regulations were designed to:

- Standardize electronic health data transactions
- Maintain privacy of personally identifiable health information
- Protect the security of such data and information

Breach: Credit Control maintains a "PHI Disclosure Log" to document any and all examples where PHI (Protected Health Information) was disclosed in error. This would include situations where medical account details were discussed with someone other than the actual patient/guarantor, third party payor, legal representative, or client. Other situations would include misdirected mail/fax/email communications containing PHI or any failure to preclude an office visitor or other unauthorized person(s) from viewing, overhearing, or otherwise obtaining access to PHI.

The Compliance Officer provides the Board of Directors with a quarterly report/analysis of compliance related issues to include a review of legal challenges filed against Credit Control and a risk assessment.

Relevant Aspects of the Control Environment, Risk Assessment, Information and Communication, Monitoring, and Control Activities

Control Environment

Credit Control strives to instil an enterprise-wide attitude of integrity and control consciousness, and set a positive tone at the top. An effective control environment is created by establishing controls surrounding the processing of information and by developing policies, which promote adherence to the requirements of the control environment.

Credit Control management is responsible for directing and controlling operations and for establishing, communicating, and monitoring control policies and procedures. Management promotes integrity and ethics through corporate values that stress the importance of proper employee conduct. Organization values and behavioral standards are communicated to all personnel through policy statements and formal codes of conduct in the employee handbook that is handed out upon hire and available on the company intranet, where employees can access many items relating to personnel and benefits.

Credit Control's organizational structure provides the overall framework for planning, directing and controlling operations. Personnel and business functions are separated into departments according to job responsibilities.

The following teams are involved in providing Credit Control's Account Management and Collection Services:

Team Name	Responsibility
Senior Management	Provides overall leadership and guidance over Account Management and Collection Services.
Information Technology	Provides support and maintenance of the network and supporting applications.

Team Name	Responsibility
Compliance	Compliance management includes training and education for staff members on applicable regulations (FDCPA, FCRA, FTC, etc.), consumer dispute/complaint tracking, litigation prevention/negotiation, quality assurance initiatives, contract development and risk management.
Medical Division Collections Manager	Manages staff of medical debt collection professionals, and monitors the way in which they handle phone calls and the letters they send to make sure the entire process operates in compliance with state and federal laws, while maximizing payments from debtors. Serves as primary liaison with three National Credit Reporting Bureaus: Transunion, Equifax and Experian.
Cable Division Collection Manager	Manages staff of telecommunication debt collection professionals and monitors the way in which they handle phone calls and the letters they send to make sure the entire process operates in compliance with state and federal laws, while maximizing payments from debtors. Serves as primary liaison with three National Credit Reporting Bureaus: Transunion, Equifax and Experian.
Support Services Manager	Focuses primarily on customer/client service, credit reporting, payment posting, consumer dispute management, client invoicing, and management of fifteen clerical support staff in two divisions. Serves as the System Administrator for credit reporting updates via E-Oscar and the consumer account verification system utilized by all three National Credit Reporting Bureaus.
Collectors	Contacts debtors via outbound/inbound phone calls and other means of communication to secure balance of debt by negotiating payment terms and methods. Adheres to FDCPA, state and federal laws/regulations.
Administrative Staff	Answers phone inquiries and directs incoming calls to various departments. Uploads new business information including demographics and financial information into collections system. Posts individual payments to debtors' accounts. Responds to debtor disputes.

Human Resources

Credit Control has formal personnel policies and procedures designed to provide that employees are qualified for their job responsibilities. Hiring policies include requiring minimum education and experience, verification of references, and extensive training. When hired, employees must sign an employment agreement that includes a confidentiality agreement covering Credit Control and client data, restricted covenants, harassment policy and acknowledgment of receipt of the employee handbook.

Credit Control Employee Training, Testing and Continuing Education Initiative

Credit Control's Employee Training, Testing and Continuing Education Initiative was developed as a three-tiered approach to further the knowledge base of employees working with consumer debt in a third party debt collection environment.

- Employee Training - Educational components of the program are designed to ensure compliance with FDCPA, FCRA, CFPB, FTC, IRS, HIPAA, etc. regulations. Collectors and specific Clerical Support Staff are required to attain an ACA Certified Collector Certificate in order to communicate with consumers regarding third party debt collection matters. The Employee Training Matrix identifies the positions required to participate in the Certified Collector Certificate program and other training initiatives. Credit Control Corporation's Employee Manual documents educational requirements. The Employee Acknowledgement Form confirms that employees are aware of the aforementioned training requirements.
- Employee Testing - Testing initiatives are conducted by Credit Control division managers in order to certify that designated employees under their direction and charge have successfully completed course requirements and prerequisites for their respective positions.
- Continuing Education - Credit Control Division Managers, the General Manager and/or the Compliance Officer are responsible for providing staff with the educational resources and regulatory updates necessary to ensure compliance with new and/or updated regulations and other operational guideline

Formal performance reviews are conducted on an annual basis at a minimum, however many employees involved in the collections process receive monthly and quarterly evaluations. Employees are evaluated on objective criteria established by management.

Risk Assessment Process

Due to the relative small size and structure of the organization, management is able to proactively identify and manage business functions and risks that could affect its ability to continue to provide services to its clients.

Through monthly manager meetings, monthly and quarterly performance evaluations, monitoring of client and customer disputes as well as a robust quality assurance function, risks are identified, analyzed, and mitigation strategies are put in place. Credit Control identifies significant risks based on management's internal knowledge of its operations and the industry in general; as well as continuous feedback from internal staff, clients, and industry subject matter experts.

Information and Communication

Credit Control is committed to maintaining effective communication with all personnel, clients and customers. To help align Credit Control's strategies and goals with operating performance, monthly manager meetings are held to disseminate relevant information and discuss the status of service delivery (collections), regulatory compliance matters (customer disputes), financial performance, security and any human resource matters. All clients have available to them contact details of relevant Credit Control team members and can reach out directly to support service managers as well as management regarding any service related matters.

Monitoring Activities

Compliance Management Program

Credit Control has developed a comprehensive Compliance Management Program administered by the Compliance Officer who reports directly to the Board of Directors. The program focuses upon:

- Compliance education and training for staff, managers, and executives on key collection related regulations

- Consumer complaint and dispute tracking
- CFPB compliance
- Internal QA processes to include recording/monitoring telephone contacts
- Consumer dispute resolution
- Disseminating federal and state regulatory advisories from the American Collectors Association
- ACA Code of Business Ethics

Consumer Support System

Credit Control created a consumer support system to establish multiple communication channels through which consumers/debtors can express concerns, complaints, compliments and suggestions regarding third party pre-collection and bad debt collection account activities conducted by Credit Control.

Management uses this information to measure the extent and impact of consumer issues in an effort to identify the nature and source(s) of consumer dissatisfaction with:

- The original creditor and/or their A/R processes
- Credit Control's contact and notification processes
- FDCPA and FCRA compliance initiatives
- Customer service standards
- Credit Control's internal efficiency in responding to consumer issues
- To identify staff training/educational needs in support of a more positive consumer experience
- To identify problematic processes and staffing resources in order to effectively resolve them

Information Technology General Control Activities

Logical Access Security

Because of the inherent risks related to managing third party records that may contain sensitive and personally identifiable information, Credit Control has stringent employment procedures governing the hiring process and placement of qualified individuals within the organization. Additionally, Credit Control has developed and maintains a documented Access Authorization Standard that governs the usage and granting of access to all Credit Control customer information and technology resources.

Access to applications is only granted to users by placing them in to a unique active directory group. Authorization of access is granted under the standards of Credit Control's Information Technology Access Control policy and Separation of Duties policy. Granting access to sensitive data is restricted by job responsibility. Department Managers notify IT immediately upon termination of an employee so that access to all systems and facilities is removed promptly.

Vendor access to the network is controlled by Credit Control.

Physical Access Security

Building access is controlled by Trilogy Proximity XP keyless entry system. All Credit Control employees are issued an RFID key card, which permits them to enter the Credit Control office. The key card is given to each employee upon employment with Credit Control and confiscated once the individual leaves the company due to termination or other reasons.

Systems Monitoring

Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems and used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system performance.

Each server is configured with audit settings that allow IT personnel to monitor server activity at the user and IP level. AlienVault Unified Security Management (USM) delivers built-in intrusion detection systems tools as part of an all-in-one security management console. It includes built-in host intrusion detection (HIDS) and network intrusion detection (NIDS) enabling Credit Control to detect threats as they emerge in on-premises infrastructure.

Secure Data Communications

Files are transferred via a secure FTP to ensure the confidentiality and security of client data. Access to the SFTP is controlled by the IT department at the request of management for new clients. Clients are restricted to their directory structure.

Change Management

Credit Control uses vendor provided software to manage, process, and store customer data. Credit Control has no access to the source code of the application(s). All patches, upgrades, and other significant changes to vendor provided software are managed by each vendor.

Redundancy, Backup and Recovery

Credit Control maintains a Security, Redundancy and Disaster Recovery Plan, and detailed application and infrastructure backup and recovery procedures.

Critical infrastructure components have been reviewed for criticality classification and assignment of a minimum level of redundancy. Weekly full-system and daily incremental backups are performed using an automated system, and backups are monitored for failure using an automated system.

Credit Control has contracted with Agility Recovery Services to permit the resumption of business operations in the event of a disaster at its data center. In a disaster situation, Agility is contracted to provide 24 mobile workstations with computers, internet connectivity and phones within 36 hours.

Scope of the System

The description of Credit Control's System for Providing Account Management and Collection Services addresses only those controls related to the administration of the customer accounts, proper recording and remittance of customer payments net of applicable fees, and compliance with applicable consumer protection regulations. The scope excludes other services and functions performed by the organization, such as Credit Controls accounting, payroll, sales, marketing, and other management functions. The description is intended to provide information for user entities and their independent auditors who audit and report on such user entities' financial statements to be used in obtaining an understanding of Credit Control's Account Management and Collection Services. The description includes certain business process controls and IT general controls that support Credit Control's services.

Subservice Organizations and Complimentary Service Organization Controls (C-SOCs)

In order to deliver its' Account Management and Collection Services, Credit Control uses subservice organizations to perform and provide various functions to support the delivery of service. The description includes only the control objectives and related controls of Credit Control and excludes the control objectives and related controls of the subservice organizations. The following is a list of subservice organizations, the services they provide, and relevant complimentary control objectives:

Subservice Organization	Description of Services	C-SOCs
Quantrax	Intelec/RMEx "smart collection" software system is used to manage all collection processes and client/consumer data and activities. A key feature is its seamless integration with dialer management. The system was developed and is supported by the Quantrax Corporation of Bethesda, MD.	Controls related to change management, functionality and availability of the RMEx system.
PaymentVision, A Division of Autoscribe Corporation	PaymentVision is a web-based application used to process customer payments.	Controls related to change management, functionality and availability of the PaymentVision system.
RevSpring	RevSpring enables Credit Control to deliver personalized financial communications through print, email, SMS, voice and web channels. RevSpring handles mailings and account notices.	Controls over the proper handling and communication with customers in accordance with applicable consumer regulations.
ICE Data Services	Checks customer accounts for bankruptcy filings/notices prior to sending account statements or other collection	Controls over the proper handling and communication with customers in accordance with applicable consumer regulations.
VoApps	Leaves a voice message without the intrusion of a call. This allows a consumer to respond at their convenience while agents stay focused on answering incoming calls instead of less efficient outbound dialing.	Controls over the proper handling and communication with customers in accordance with applicable consumer regulations.

Complementary User-Entity Controls

Credit Control Corporation uses subservice organizations to perform various functions to support the delivery of services. The scope of this report does not include the controls and related criteria at the subservice organizations.

In designing its services, the service organization (Credit Control Corporation) has contemplated that certain complementary user-entity controls would be implemented by the user organization to achieve certain control objectives in the report. The list of complimentary user-entity controls noted below is not and should not be considered a comprehensive list of all controls that should be employed by user-entities. Other controls may be required.

User entities of Credit Control Corporation's system should maintain controls to provide reasonable assurance that:

1. Physical and logical access to Credit Control Corporation's systems, using terminals at customer locations, is restricted to authorized individuals.
2. User-entities protect passwords used to access the Credit Control Corporation portal to update and change account information.
3. Breaches in security at user-entities which may impact the account collection process are promptly communicated to Credit Control Corporation.
4. Changes to authorized employees at user-entities are communicated to Credit Control Corporation in a timely manner so that access may be removed.
5. User-entities are responsible for periodically reviewing authorized users and their associated access privileges.
6. The process of deciding which customer personnel need specific functionality and the execution of granting this functionality is the responsibility of the user-entity.
7. User-entities must send data in an encrypted manner using industry standard encryption or request that the Credit Control provide a secure transmission method.
8. User-entities are responsible for ensuring the accuracy of the information provided to service organization for delinquent debt recoveries.
9. User-entities must make certain the debts owed are accurate and past due.
10. User-entities should have approval by proper authority to list the debt with service organization and ensure that the debtor has not been discharged in bankruptcy.

SECTION IV

CONTROL OBJECTIVES, RELATED CONTROLS, AND TESTS OF OPERATING EFFECTIVENESS

Description of Controls

The Trust Services Principles, related criteria, and Credit Control Corporation's related controls are an integrated part of the management's system description and are included in this section for presentation purposes. The Reporting Period used within this report throughout the period June 1, 2018 to May 31, 2019 ("Reporting Period").

Information provided by the Service Auditor

We included the description of the tests performed to determine whether the controls were operating with sufficient effectiveness to achieve the specified criteria and the results of the tests of controls, as specified below.

Our tests of the control environment included the following procedures, to the extent we considered necessary: (a) inspection of Credit Control Corporation's Account Management and Collection Services System; (b) inquiry with management, operations, administrative and other personnel who are responsible for developing, monitoring, and execution of controls; (c) observations of personnel in the performance of controls; (d) inspection of documents and records pertaining to controls; (e) inquiry and inspection of compliance monitoring; (f) inquiry and inspection of human resources and information security policies. Additionally, observation and inspection procedures were performed as it relates to system generated reports and queries, to assess the completeness and accuracy (reliability) of the information utilized in the performance of our testing of the control activities.

Control Objective 1 – Controls Provide Reasonable Assurance that New Clients are Setup in the System Completely and Accurately.

Ref	Credit Control Corporation Controls Description	PBMares Tests of Controls	Test Results
1.01	The company ensures a signed contract exists that details the nature of the services to be provided prior to setup within the system.	**Inspection** For a sample of active clients during the Reporting Period, inspected evidence to determine whether a formally documented signed contract exists that details the nature of the services to be provided prior to being set up in the system.	No exceptions noted.
1.02	The company uses a standardized "New Client Form" to capture significant attributes of the client and applicable contract terms.	**Inspection** For a sample of active clients during the Reporting Period, inspected evidence of the corresponding "New Client Form" to determine whether the form was formally documented and completed to capture significant attributes of the client and applicable contract terms.	No exceptions noted.
1.03	New clients are setup in the system by the COO. Master client flies are matched to the New Client form to ensure accuracy.	**Inspection** For a sample of active clients during the Reporting Period, inspected evidence of the corresponding "New Client Form" and the client's system access to verify the client's account was appropriately authorized and that system access was setup appropriately in the RMEx system.	No exceptions noted.
1.04	Access to setup and modify client files is restricted to individuals who have appropriate authority to do so.	**Inspection** Inspected evidence of the RMEx system user list to determine whether access to setup and modify client files is appropriately restricted to a limited number of individuals with direct job responsibility.	No exceptions noted.

Control Objective 1 – Controls Provide Reasonable Assurance that New Clients are Setup in the System Completely and Accurately (Continued)

Ref	Credit Control Corporation Controls Description	PBMares Tests of Controls	Test Results
1.05	The company uses a third party software (RMEx), to setup, load and process client files. The programming to load the files was created by the vendor.	**Inquiry** Performed corroborative inquiry of Management and IT personnel to verify that the company does not have access to the RMEx source code.	No exceptions noted.
1.06	The company does not have access to modify code to the software.	**Inquiry** Performed corroborative inquiry of Management and IT personnel to verify that the company does not have access to the RMEx source code.	No exceptions noted.
1.07	The company has a vendor management process which oversees the services provided by all critical vendors. Key vendor management controls include: - Reviewing contract for applicable CIA terms - Reviewing applicable financial reports - Reviewing applicable SOC Reports	**Inquiry and Inspection** Inspected evidence of a formally documented list of all critical vendors maintained by Management. Performed corroborative inquiry of Management to determine if the company has a formal vendor management process to oversee the services provided by critical vendors. Inspected evidence of Management's formally documented vendor management policy and evidence of Management's review over all critical vendor contracts for applicable CIA terms, financial reports, and SOC reports to determine that Management has a formally documented policy and is following the policy in practice with all critical vendors identified.	No exceptions noted.

Control Objective 2 – Controls Provide Reasonable Assurance that Payments are Processed Timely and Accurately.

Ref	Credit Control Corporation Controls Description	PBMares Tests of Controls	Test Results
2.01	Files are transferred via a secure FTP to ensure the confidentiality and security of client data.	**Inquiry and Inspection** Inquired of management as to the nature of incoming and outgoing files transferred via the secure FTP server. Inspected evidence of server settings and configurations to verify the server has been properly secured and client files are properly segregated from that of other clients to ensure the confidentiality and security of client data.	No exceptions noted.
2.02	Each morning (as applicable), clerical associate receives an email notifying them that a client has uploaded a new file. New files consists of payments made to the client, new business/placements and any applicable recalls (due to aging or other criteria).	**Observation and Inspection** For a sample selection of days, observed a copy of the email notification notifying the clerical associate of a new file uploaded by a client. Observed the associate download all files received for that day to ensure the notifications include payments, new business, and applicable recalls.	No exceptions noted.
2.03	Clerical load the file into the RMEx system via a script developed by the vendor.	**Observation and Inspection** For a sample selection of days, observed the clerical associate load all received files from that morning into the RMEx system. Inspected the incoming file and selected a sample of incoming postings to ensure the selected postings agree to the system data after being loaded into RMEx to verify the data was properly imported.	No exceptions noted.
2.04	Clerical runs an edit/check report looking for duplicates, bad addresses, incorrect balances or missing information. Errors are resolved to ensure the loaded file matches the raw data file provided by the client.	**Observation and Inspection** For a sample selection of days, observed the clerical associate run an edit/check report to ensure the check looks for duplicates, bad addresses, incorrect balances or missing information. Inspected the error log and determine if a resolution was completed for any identified errors.	No exceptions noted.

Control Objective 2 – Controls Provide Reasonable Assurance that Payments are Processed Timely and Accurately. (Continued)

Ref	Credit Control Corporation Controls Description	PBMares Tests of Controls	Test Results
2.05	Contracts and SLAs with third party vendors govern and address CIA commitments to ensure the confidentiality, integrity and availability of the services provided for account scrubbing (checking for bankruptcies, etc.) and collection letters, respectively.	**Inspection** For a sample selection of third party vendors, inspected a copy of the signed contract and SLA to ensure the confidentiality, integrity and availability of the services provided for account scrubbing and collection letters.	No exceptions noted.
2.06	Payments received in the mail are processed by clerical staff daily as part of batch processing procedures.	**Observation** For a sample selection of days, observed the clerical associate perform the daily processing and posting of all incoming checks to determine that once loaded, the payments are processed as part of the daily batch.	No exceptions noted.
2.07	All payments are processed via a third-party (Payment Vision). Clerical receives a daily lock-box file via SFTP indicating all payments received. The file notates the necessary information to verify and validate a customer payment.	**Observation and Inspection** For a sample selection of days, observed the clerical associate receive the daily lock-box file via sFTP indicating all payments were received and inspected the file to verify the file lists the necessary information for each payment to validate a customer payment was processed.	No exceptions noted.

Control Objective 3 – Controls Provide Reasonable Assurance that Reporting to Clients is Accurate, Submitted Timely, and in Accordance with Contract Requirements.

Ref	Credit Control Corporation Controls Description	PBMares Tests of Controls	Test Results
3.01	In accordance with the contact terms the following standard reports can be made available to client upon the clients request. Activity History Status Report Placement History Close-out Regression Acknowledgement Statement These reports can be made available to the client normally via Mail or Email. The reports can also be placed on the client's secure FTP server or placed on Credit Controls secure FTP server if needed. Other specialized reports may be produced for the client on a case by case basis.	**Inspection** Inspected email and SFTP documentation to verify documents are sent to clients securely detailing balances and payments made.	No exceptions noted.
3.02	Administrative and clerical prepares invoices in accordance with the contract terms. The CFO reviews the invoice to ensure the total payments and total commissions are accurate.	**Inspection** Inspected invoices for notations of review and preparation in accordance with contract terms prior to delivery to the client.	No exceptions noted.
3.03	For payments to customers processed via check, appropriate segregation of duties exist over the disbursement process.	**Observation** Observed the processing and remittance of monthly invoices, as well as check payments to verify controls are performed as stated. Additionally, observed the processing and remittance of daily reports, as well as ACH payment to verify controls are performed as stated.	No exceptions noted.
3.04	For payments to customers processed via wire, appropriate segregation of duties exist over the ACH transaction posting.	**Observation** Observed the processing and remittance of monthly invoices, as well as check payments to verify controls are performed as stated. Additionally, observed the processing and remittance of daily reports, as well as ACH payment to verify controls are performed as stated.	No exceptions noted.

Control Objective 4 – Controls Provide Reasonable Assurance that the System's Availability Commitments and System Requirements are met.

Ref	Credit Control Corporation Controls Description	PBMares Tests of Controls	Test Results
4.01	Critical infrastructure components have been reviewed for criticality classification and key systems are appropriately configured for periodic full backups.	**Inquiry and Inspection** Inquired of management and observed the data center, backup facility, and other network equipment to verify a minimum level of redundancy has been implemented. Inspected screenshots to verify key systems are configured for periodic full backups.	No exceptions noted.
4.02	Backups are monitored for failures and are investigated and resolved in a timely manner.	**Inspection** For a sample selection of days, inspected the backup notification successes and failures. For any backup failures, inspected evidence to confirm the backup failure was resolved timely.	No exceptions noted.
4.03	The tape backups are transported and stored offsite.	**Inquiry and Inspection** Inquired of management and confirmed tape backups are transported offsite daily and stored at a secured facility. For a sample selection of days, inspected documentation to verify tape backups were taken offsite daily to the secured facility.	No exceptions noted.
4.04	The entity has contracted with a third-party recovery facility to permit the resumption of IT operations in the event of a disaster at its data center.	**Inspection and Inquiry** Inquired of management as to third party recovery facilities used in the event of a disaster at the firm's data center. Inspected the contract and SLA with the third-party recovery facility to verify stated services are covered.	No exceptions noted.
4.05	Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems and used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity.	**Inspection** Inspected the configurations of logging and monitoring software to verify monitoring is enabled and appropriately set to monitor for system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity.	No exceptions noted.

Control Objective 4 – Controls Provide Reasonable Assurance that the System's Availability Commitments and System Requirements are met. (Continued)

Ref	Credit Control Corporation Controls Description	PBMares Tests of Controls	Test Results
4.06	Vulnerability scans are performed annually and their frequency is adjusted as required to meet ongoing and changing commitments and requirements.	**Inquiry and Inspection** Inquired of management to confirm vulnerability scans are performed on an annual basis, and any vulnerabilities identified are researched and resolved within a timely manner. Inspected documentation of the vulnerability scans performed to confirm the scans were performed annually. Confirmed through inquiry that management risk rates any vulnerabilities identified and resolves critical and high risk items within a timely manner.	No exceptions noted.
4.07	Antivirus software is configured to receive an updated virus signature at least daily. A network operation receives a report of devices that have not been updated and follows up on the devices.	**Inspection** Inspected the antivirus configurations in place to verify the antivirus software is set to receive an updated virus signature at least daily. Inspected antivirus reports identifying devices that were not updated and verified each case was reasonable, as well as researched and resolved within a timely manner.	No exceptions noted.
4.08	Antivirus software is installed on workstations, laptops, and servers supporting such software.	**Inspection** Inspected the antivirus configurations in place to verify antivirus software is installed on all workstations, laptops, and servers.	No exceptions noted.

Control Objective 5 – Controls Provide Reasonable Assurance Regarding the Physical and Logical Security of the System and its Components.

Ref	Credit Control Corporation Controls Description	PBMares Tests of Controls	Test Results
5.01	Policy and procedures documents for significant processes are formally documented and available on the company's network; updates are made as needed.	**Inspection** Inspected the company network diagram to verify that policies and procedures are formally documented, posted, and available as stated.	No exceptions noted.
5.02	Roles and responsibilities are defined in formally documented job descriptions and communicated to managers and their supervisors.	**Inquiry and Inspection** Inquired of management to verify all job descriptions are communicated to managers and supervisors. Inspected the job descriptions to verify that all positions have been formally documented and include roles and responsibilities.	No exceptions noted.
5.03	Job descriptions are reviewed on a periodic basis for needed changes and updated if such changes are identified.	**Inquiry and Inspection** Inquired of management to verify job descriptions are reviewed on at least an annual basis and updated as stated. Inspected evidence to confirm the job descriptions were reviewed annually and updated for required changes.	No exceptions noted.
5.04	Personnel are required to read and accept the entity's code of conduct and the statement of security, confidentiality, and privacy practices within 30 days of hire date and in the event of a subsequent policy change.	**Inspection** For a sample selection of employees and new hires, inspected the employee's signed code of conduct. Verified personnel are required to read and accept the entity's code of conduct and the statement of security, confidentiality, and privacy practices within 30 days of hire date and in the event of a subsequent policy change.	No exceptions noted.
5.05	Personnel are required to attend annual security, confidentiality, and privacy training.	**Inspection** Inspected the training attendance sheet to verify all eligible employees attended the annual security training.	No exceptions noted.
5.06	Complex password settings are enforced on all systems and supporting technology layers, and system security is configured to require users to change their password every 90 days.	**Inspection** Inspected company policy and system settings to determine whether policy requirements are met by the system password settings in place.	No exceptions noted.

Control Objective 5 – Controls Provide Reasonable Assurance Regarding the Physical and Logical Security of the System and its Components. (Continued)

Ref	Credit Control Corporation Controls Description	PBMares Tests of Controls	Test Results
5.07	Requests for new user accounts, or modifications to existing accounts are submitted and approved prior to provisioning employee, contractor, and service access to systems.	**Inspection** For a sample of new hires, inspected the access modification request and subsequent approval as well as the user access list to verify access was appropriately requested, approved, and granted in the system in accordance with the approved request.	**Exception Noted.** For 2 of 6 new users selected for testing, there was no formal evidence documenting the specific access rights requested to be setup across the various technology layers within Credit Control's environment, along with the appropriate management approval, prior to provisioning the access.
5.08	Roles and access rights are reviewed by Management whenever an employee position changes. Access change requests resulting from the review are submitted to the IT Department for review and implementation.	**Inspection** For a sample of transfers, inspected the access modification request and subsequent approval as well as the user access list to verify access was appropriately requested, approved, and granted in the system in accordance with the approved request.	No exceptions noted.
5.09	Upon termination or resignation, the employee's manager or HR immediately notifies the IT department to revoke all system and badge card access. Upon notification, access is removed within a timeline set by the corporate policy.	**Inspection** For a sample of terminated employees, inspected the termination notification to confirm the termination notification was sent timely. Additionally, inspected the user access listings to verify that access has been appropriately disabled as requested.	No exceptions noted.
5.10	System access is restricted through the use of security groups, and privileged user accounts are established and administered to authorized individuals only based on direct business need.	**Inquiry and Inspection** Inquired of management to verify system access is restricted through the use of security groups, and privileged user accounts are established and administered to authorized individuals only based on direct business need. Inspected system listings to determine appropriate persons have external access to the network. Additionally, inspected VPN configuration settings to verify that access has been properly secured.	No exceptions noted.

Control Objective 5 – Controls Provide Reasonable Assurance Regarding the Physical and Logical Security of the System and its Components. (Continued)

Ref	Credit Control Corporation Controls Description	PBMares Tests of Controls	Test Results
5.11	Privileged client accounts are created based on a written authorization request from the designated client point of contact. These accounts grant access to the Quantrax system by the client. Access is restricted to view only.	**Inspection** Inspected the RMEx client access listing and reviewed written authorization requests for a sample selection of clients to confirm access was formally requested and approved prior to system access being granted.	No exceptions noted.
5.12	User access reviews over systems and supporting technology layers are performed on a periodic basis.	**Inquiry and Inspection** Performed corroborative inquiry of management and verified that user access reviews are performed annually. Additionally, inspected a copy of the annual user access review to determine the review was performed timely by an appropriate individual.	No exceptions noted.
5.13	On a periodic basis all firewall configurations are reviewed to ensure alignment with corporate policies and approved by appropriate personnel.	**Inquiry and Inspection** Inquired of management to verify firewall configuration reviews are performed annually. Inspected the annual firewall review to determine the review was performed timely by an appropriate individual.	No exceptions noted.
5.14	Processes are monitored through automated checks and manual adhoc spot checks. Results are shared with applicable personnel and customers, and actions are taken and communicated to relevant parties.	**Inspection** Inspected the most recent internal and external vulnerability scans to verify that scans occur as stated by company policy to identify vulnerabilities through spot checks, and that appropriate actions are taken to remediate any issues identified.	No exceptions noted.
5.15	External access by employees is permitted only through encrypted connections and is limited to IT personnel.	**Inspection** Inspected external access permissions to verify only IT personnel have permissions to use encrypted, external connections to the network.	No exceptions noted.

Control Objective 5 – Controls Provide Reasonable Assurance Regarding the Physical and Logical Security of the System and its Components. (Continued)

Ref	Credit Control Corporation Controls Description	PBMares Tests of Controls	Test Results
5.16	VPN, SSL, secure file transfer program (SFTP), and other encryption technologies are used for defined points of connectivity and to protect communications between the Company and its clients.	**Inspection** Inspected configuration settings for VPN, SSL, and SFTP to verify they are properly configured to provide secure point of connectivity to protect communications between the company, its clients, and its vendors.	No exceptions noted.
5.17	An intrusion prevention system is in place and continuously monitors for potential malicious activity and intrusion.	**Observation and Inspection** Observed the intrusion prevention tool in place to determine its existence and configurations in place. Inspected the tool to confirm it is configured appropriately to monitor for potential malicious activity and intrusion.	No exceptions noted.
5.18	The company has an extensive training process, certified by the ACA, which candidates for employment must pass.	**Inspection** For a sample selection of employees, inspected the employee ACA Certification to ensure company policy training requirements were met.	No exceptions noted.

Control Objective 6 – Controls Provide Reasonable Assurance that the Confidentiality of the Client and its Customer's Data is Maintained.

Ref	Credit Control Corporation Controls Description	PBMares Tests of Controls	Test Results
6.01	Communication information is located within the Employee Handbook for internal users to confidentially report security concerns or complaints to appropriate individuals.	**Inspection** Inspected the employee handbook to verify communication information is appropriately available to employees.	No exceptions noted.
6.02	External points of connectivity are protected by a firewall complex.	**Inspection** Inspected the network topology to verify that the design of the network includes implementation of an appropriate firewall complex to help protect internal resources and communications.	No exceptions noted.
6.03	VPN, SSL, secure file transfer program (SFTP), and other encryption technologies are used for defined points of connectivity and to protect communications between the Company and its clients.	**Inspection** Inspected the configuration settings for the VPN, SSL, and SFTP to verify they are properly configured to provide secure point of connectivity to protect communications between the company, its clients, and its vendors.	No exceptions noted.
6.04	Backup media are encrypted during retention.	**Inspection** Inspected backup configurations to verify that backup data is encrypted during retention.	No exceptions noted.
6.05	USB devices and removable media are not allowed to connect to workstations.	**Inspection** Inspected storage settings to verify that the installation of removable media devices is not enabled.	No exceptions noted.
6.06	Formal information sharing agreements are in place with related parties and vendors. These agreements include confidentiality commitments applicable to that entity.	**Inquiry and Inspection** Inquired of management to determine critical vendors. Inspected the information sharing agreements to verify their existence with related parties and vendor, as well as confirm the agreements include confidentiality commitments applicable to the entity.	No exceptions noted.

Control Objective 6 – Controls Provide Reasonable Assurance that the Confidentiality of the Client and its Customer's Data is Maintained. (Continued)

Ref	Credit Control Corporation Controls Description	PBMares Tests of Controls	Test Results
6.07	Secure FTP is used to transfer client files that contain sensitive information to ensure security and confidentiality, and FTP configurations are appropriately restricted.	**Inquiry and Inspection** Inquired of management as to the nature of incoming and outgoing files transferred through and stored on the FTP server. Inspected server settings and configurations to verify the server has been properly secured and client files are properly segregated from that of other clients.	No exceptions noted.
6.08	The preferred method of sending sensitive information to clients is secure FTP however, in some instances secure FTP is not available. In these instances a secure email or an email with an encrypted attachment is used to transmit the data.	**Inquiry and Inspection** Inquired of staff to verify employees are aware of secure file transfers methods available in the event that the secure FTP is unable to be used to transmit sensitive or confidential information. Inspected the tools available to employees, confirming users have the ability to encrypt attachments and send secure emails.	No exceptions noted.

Control Objective 7 – Controls Provide Reasonable Assurance that Data Integrity is Maintained through the System Development Lifecycle.

Ref	Credit Control Corporation Controls Description	PBMares Tests of Controls	Test Results
7.01	Critical software necessary to the system are supplied by vendors. These vendors are responsible for having appropriate configuration management and change management controls and procedures in place. The company evaluates this compliance via the use of SOC reports or other model validation reports.	**Inquiry and Inspection** Inquired of management to determine the list of critical vendors during the reporting period. Inspected the manual list of critical vendors to verify existence of a formally documented list of critical vendors classified by risk. For a sample selection of critical vendors, obtained the contracts, other agreements, financial reports, and SOC reports, as applicable. Inspected Management's evaluation over each critical vendor selected to determine that the vendors have appropriate configuration management and change management controls and procedures in place.	No exceptions noted.
7.02	Attestation reports (SOC 2 reports) are obtained and evaluated when available for critical vendors.	**Inspection** For a sample selection of critical vendors, inspected the SOC attestation reports as well as management's formal evaluation over the SOC reports, to determine that a SOC report is in existence and was obtained, and that management performed annual due diligence over critical vendors.	No exceptions noted.
7.03	Prior to applying a vendor upgrade or load program change an approval is provided by the company to the vendor.	**Inspection** Inspected change tickets to verify the change was appropriately requested, documented, tested, and approved prior to migration to production.	No exceptions noted.

Control Objective 7 – Controls Provide Reasonable Assurance that Data Integrity is Maintained through the System Development Lifecycle. (Continued)

Ref	Credit Control Corporation Controls Description	PBMares Tests of Controls	Test Results
7.04	Access to apply changes to the production system is restricted to appropriate individuals only with direct job responsibilities.	**Inquiry and Inspection** Inquired of management to verify that access to install applications is restricted to authorized IT personnel. Inspected the user access listings to determine that access to apply changes to production is appropriately restricted to a limited number of individuals based on direct job responsibility.	No exceptions noted.
7.05	Vendor access to the system is limited to the specific device/application supplied by the vendor. This access is controlled by IT management.	**Inquiry and Inspection** Inquired of management and verified that vendor access is controlled and restricted as stated. Inspected the user access listings to determine that vendor access to the system is appropriately restricted, and provisioning of access is controlled by a limited number of authorized individuals within the IT department.	No exceptions noted.
7.06	Before a client goes live in the system, the Company works with the client to review the file layout and required data fields. The vendor loads the files into Quantrax. The COO runs error reports to verify the accuracy of the system data matches the raw data file. Once the COO has confirmed files are being loaded correctly, the client is ready to be put into live production.	**Inquiry and Inspection** Inquired of management and verified that all new clients go through the change management process to go live in the system. Inspected a sample selection of change tickets to verify the change request was formally documented, tested, and approved prior to migration to production. Additionally, verified as part of the testing process, the COO runs the error reports to verify the accuracy of the system data.	No exceptions noted.

Control Objective 8 – Controls Provide Reasonable Assurance that Compliance and Regulatory Activities are Monitored and Resolved.

Ref	Credit Control Corporation Controls Description	PBMares Tests of Controls	Test Results
8.01	All consumer complaints and disputes are formally logged, tracked, researched, and resolved by the compliance officer.	**Inquiry and Inspection** Inquired of the compliance officer and inspected the complaint log, to verify all consumer complaints and disputes are formally logged, tracked, researched and resolved by the Compliance Officer.	No exceptions noted.
8.02	Once an investigation is completed, the Compliance Officer responds to the consumer via the CFPB portal; advising them of details pertinent to the account(s) in question and answering questions/concerns expressed by the consumer.	**Inquiry, Observation, and Inspection** Inquired of the compliance officer and inspected the complaint log to determine that complaints are resolved in a timely manner. Observed onsite the CFPB portal to verify the Compliance Officer responds to the consumer once the investigation is completed, and advises them of the details pertinent to the account(s) in question and answers all questions and concerns communicated by the consumer.	No exceptions noted.
8.03	The Compliance Officer provides a compliance report to the board to report any legal issues.	**Inquiry and Inspection** Inquired of the Compliance Officer to confirm a compliance report is provided to the board to report any legal issues on a quarterly basis. Inspected the complaint log, ACA training materials, and a sample of quarterly compliance reports issued to the board to determine that Management designs controls to ensure compliance with applicable laws and regulations via: training programs, in-house counsel, and review of customer complaints.	No exceptions noted.

Control Objective 8 – Controls Provide Reasonable Assurance that Compliance and Regulatory Activities are Monitored and Resolved. (Continued)

Ref	Credit Control Corporation Controls Description	PBMares Tests of Controls	Test Results
8.04	Internal QA managers monitor telephone calls and letters of the collection staff to verify compliance with state and federal regulations.	**Inquiry and Observation** Inquired of the compliance officer and the manager on the floor to determine that QA managers are available during the day to monitor telephone calls and letters of the collection staff. Observed one QA manager continuously jump onto the calls of various collectors on the floor to ensure compliance with state and federal regulations.	No exceptions noted.
8.05	Compliance education and training is provided for staff, managers, and executives on key collection related regulations.	**Inquiry and Inspection** Inquired of the compliance officer and the CFO to confirm the compliance education and training requirements for staff. For a sample selection of employees who are required to complete the training, inspected the training certificates of completion to determine that appropriate personnel are receiving the required compliance education related to regulations.	No exceptions noted.

SECTION V

OTHER INFORMATION PROVIDED BY CREDIT CONTROL CORPORATION (UNAUDITED)

Management's Response to Results of Tests Performed

The following information documents Credit Control Corporation's management response to the results of tests performed by PBMares, LLP in Section IV of this report.

Control	Test Procedures	Results	Management's Response
Control #5.07: Controls provide reasonable assurance regarding the physical and logical security of the system and its components.	**Inspection** For a sample of new hires, inspect the access modification request and subsequent approval as well as the user access list to verify access was appropriately requested, approved, and granted in the system in accordance with the approved request.	**Exceptions noted.** For 2 of 6 new users selected for testing, there was no formal evidence documenting the specific access rights requested to be setup across the various technology layers within Credit Control's environment, along with the appropriate management approval, prior to provisioning the access.	Credit Control Corporation acknowledges a formal new access provisioning process was in place during the report period, but the specific system access rights to be provisioned along with the appropriate management approval was not always formally documented prior to the system access being setup. However, access to provision new system access is limited to a restricted number of system administrators who are in a position to know what access to provision. System administrators work closely with HR and the hiring manager on what access to add across the supporting technology layers. Management has subsequently implemented a formal new access provisioning form for new employees as well as existing employees who require modifications in system access, and has retrained all employees on the new user provisioning process to ensure adherence to the new process.