CorporateAmerica
CREDIT UNION
DIFFERENT STARTS HERE™

2019

DUE DILIGENCE

REPORT

CorporateAmerica CREDIT UNION

DIFFERENT STARTS HERE™

2019 DUE DILIGENCE REPORT

TABLE OF CONTENTS

INFORMATION SECURITY

Corporate America Credit Union (CACU) realizes the importance of the appropriate management and protection of our physical and informational assets. The following information is intended to provide transparency into CACU's approach to its information security program and to assist our member credit unions with their due diligence and compliance with National Credit Union Administration (NCUA) Rules and Regulations.

CACU maintains the following information security infrastructure:

Information Security Management System
CACU assigns the highest precedence on security and utilizes technology/human security measures to protect all information within its network. Our Information Security Management System includes protecting information in all forms - written, spoken, at rest, recorded electronically, printed and stored on network devices. CACU protects all information from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle.

Security Policy
The CACU corporate network is regularly tested for weaknesses to improve the security of those systems. Independent security firms are contracted to perform internal and external vulnerability tests. Dell SecureWorks is utilized for our Intrusion Prevention System. Firewalls are used to protect our internal network and are continuously monitored for unauthorized traffic. Network Security Maintenance is performed daily for new vulnerabilities uncovered by major software vendors.

Data Destruction
Portable media, hard drives, tablets, cell phones and any portable media no longer in use by CACU are stored in a secure room and destroyed on annual basis to prevent data leakage or theft.

Data Classification
Protected information is classified into one of three sensitivity levels or classifications:

- **Confidential Data -** Confidential data is highly sensitive and may have personal privacy considerations, or may be restricted by federal or state law. The highest levels of security controls are applied to confidential data. Data is classified as Confidential when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to CACU or its members. Access to Confidential data is controlled from creation to destruction, and is granted only to those persons affiliated with CACU who require such access in order to perform their job ("need-to-know"). Access to Confidential data is individually requested and then authorized by the Data Owner who is responsible for the data. Examples of Confidential/Restricted data include financial data, Social Security and credit card numbers, and individuals' personal information.

- **Internal/Private Data -** Data is classified as Internal/Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to CACU or its members. By default, all information assets that are not explicitly classified as Confidential or Public data should be treated as Internal/Private data. Reasonable levels of security controls are applied to Internal/Private data. Access to Internal/Private data is requested from, and authorized by, the Data Owner who is responsible for the data. Access to Internal/Private data may be authorized to groups of persons by their job classification or responsibilities ("role-based" access), and may also be limited by one's department. Internal/Private Data is moderately sensitive in nature. Often this data is used for making decisions, and therefore it is important this information remain timely and accurate. The risk for negative impact on CACU should this information not be available when needed is typically moderate. Examples of Internal/Private data include official CACU records such as financial reports, human resources information, some research data, unofficial records, and budget information.

- **Public Data -** Data is classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to CACU or its members. Public data is not considered sensitive; therefore, it may be granted to any requester or published with no restrictions. The impact on CACU should Public data not be available is typically low (inconvenient but not debilitating). Examples of Public data include directory information, press releases, and research publications.

Examples of pre-defined types of confidential information:

- Personally Identifiable Financial Information (PIFI) - Covered under the Gramm-Leach-Bliley Act (GLBA)

  For the purpose of meeting security breach notification requirements, PIFI is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

  - Social Security number
  - State-issued driver's license number
  - Date of birth
  - Financial account number in combination with a security code, access code or password that would permit access to the account
  - Information collected about the customer obtained in connection with providing the financial product or service. that would permit access to the account
  - Information collected about the customer obtained in connection with providing the financial product or service.

- Payment Card Information - Covered under PCI DSS

  Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

  - Card holder name
  - Service code
  - Expiration date
  - CVC2, CVV2 or CID value
  - PIN or PIN block
  - Contents of a credit card's magnetic stripe

Data Handling Requirements
Information classified as "Confidential" and "Internal/Private" is protected in both electronic and physical form. Electronically, role based access controls are used to restrict access to the protected information. In physical form the data is marked as to the level of protected information and physical access to the information is restricted by the owner of the physical media.

Public data is unrestricted and this level of protection shall be the default for any unmarked media.

External Audits
On an annual basis, CACU engages an outside auditor to perform an assessment of its infrastructure security and vulnerabilities. CACU continued with TraceSecurity to perform the remaining audits items designated in 2018. CACU has scheduled audits to begin in late March of 2019. These audits will include: Onsite/Remote Social Engineering, an Onsite IT Audit, Security Assessment of Network Vulnerabilities, and External and Internal Penetration tests.

INCIDENT RESPONSE

CACU understands the significance of reporting security incidents and breaches and has an Incident Response Plan ensuring suspicious and criminal activities related to electronic communication and data are reported and investigated promptly. Our plan not only applies to our employees but also to contractors and third party vendors who process, store, transmit, or have access to any CACU information or computing equipment.

NCUA 12 CFR Part 748 Appendix A & B requires credit unions to establish a security breach response program and, in general, to notify affected members when a breach occurs. Additionally, credit unions are responsible for ensuring that third party service providers take appropriate measures designed to meet the objectives of the guidelines and comply with Section 501(b) of GLBA.

CACU's incident response program is one component of our overall information security program. Key elements to our response program include a response team, member notification and assistance process, third party service provider implications, and cooperation with law enforcement and regulatory agencies. third party service provider implications, and cooperation with law enforcement and regulatory agencies.

BUSINESS CONTINUITY AND DISASTER RECOVERY

CACU is committed to providing uninterrupted services to our members under normal and adverse conditions and, therefore, under the guidance of the Board of Directors and management, addresses business continuity planning responsibilities with an enterprise-wide perspective by considering technology, business operations, communication, and testing strategies for the entire credit union.

The Board of Directors has appointed a senior level Business Continuity Planning (BCP) Committee representing multiple operational areas to oversee business continuity planning in order to establish the support and culture to ensure its effectiveness. The BCP Committee ensures procedures are developed and kept current with changes in potential threats, the business environment, critical business processes or systems.

CACU's BCP ensures the sustainability of critical business processes at a level acceptable to the business, our partners, and members. The BCP has been designed to address and incorporate the guidance provided by the Federal Financial Institutions Examination Council (FFIEC), as well as the input from the NCUA.

As part of continuous improvement for our Business Continuity Plan including Disaster Recovery, the following is performed on annual basis:

- **Business Impact Analysis (BIA) –** The BIA scope evaluates all business processes and identifies processes that could significantly impact continued operations (critical) and determines how long the organization can continue to function without each critical process.

- **Formal Risk Assessment –** A risk assessment is performed for each business process classified as critical by the BIA and identifies and documents potential risks and mitigation of such risk.

- **Review of Business Continuity Strategies –** Strategies are reviewed for each critical business process.

- **Pandemic Preparedness –** A separate plan is maintained as part of CACU's BCP addressing situations that may arise in the event of a pandemic influenza threat. This plan addresses and incorporates the guidance provided by the FFIEC, as well as the guidance from the NCUA. The plan is documented, tested, and reviewed as part of our Business Continuity Program.

- **Exercise and Maintain the Plan –** All critical business processes are tested on an annual basis or within three months after significant changes in business processes, technology or the plan.

Physical and Environmental Controls

Locations	Physical & Environmental Controls
Corporate Headquarters (Irondale)	Fire Suppression, Backup Generator, Uninterruptible Power Supply, Electronic Controlled Access, Redundant Internet Connections for automatic failover
Primary Datacenter (Homewood)	Fire Suppression, HVAC Redundancy, Backup Generators, Uninterruptible Power Supply, Electronic Controlled Access, Redundant Internet Connections for automatic failover
Secondary Datacenter (Azure DRaaS)	Fire Suppression, HVAC Redundancy, Backup Generators, Uninterruptible Power Supply, Electronic Controlled Access, Redundant Internet Connections for automatic failover, Local Redundant Storage (LRS)

An alternate work site is available in Clanton, Alabama and is utilized as alternate operations site in the event our headquarters becomes unavailable or not accessible.

Technology Infrastructure

CACU deploys virtual technology to support and maintain its primary and secondary datacenters. Utilizing replication technology ensures our critical systems are constantly being replicated and backed up to our secondary datacenter. In the event of loss of our primary datacenter, our secondary datacenter would be activated and become our primary datacenter. All member facing applications and communications would be available within four hours if the primary datacenter was lost.

Systems Testing

In order to be able to provide service to our members in the event of a disaster, CACU has developed the Business Continuity and Disaster Recovery Program based on risk. Our process requires us to determine risk and mitigate those risks. On an annual basis every business process conducts a Business Impact Analysis and uses this to modify or validate the Business Continuity Plan. The plans are tested using table top, partial and full failover exercises.

The CACU Information Technology (IT) staff performs testing of the overall disaster recovery plan for the organization at least annually. In addition to the disaster recovery plan, IT staff maintains step-by-step plans in case of disaster. The entire IT staff is trained to access and execute the Business Continuity Plan including Disaster Recovery.

Testing Status

December 2018 to January 4, 2019:

CACU has migrated its tier one applications and communications to Azure Disaster Recovery as a Service. CACU was able to stage a complete failover to a test environment over a four week period. This allowed no down time to our membership during testing and migration of tier one applications and communications. Testing completed successfully. The migration to Azure has allowed CACU to be have a more robust disaster recovery infrastructure. Disaster Recovery documentation is being finalized and a full disaster recovery test is scheduled for June 2019.

VENDOR MANAGEMENT

CACU has established and implemented appropriate service provider management over each significant service provider relationship to include risk assessment/planning, due diligence, contract review and ongoing monitoring of the service provider's performance.

Periodic performance reviews and risk assessments are conducted for new and existing contract service providers to determine if the relationship helps CACU achieve our strategic and financial goals. These assessments also allow us to not only identify risks but ensure these risks have been properly mitigated through the implementation of the requirements found in NCUA 12 CFR Part 748, Appendix A.

Performance reviews are scheduled based on the service provider's classification. The scope and depth of the performance review and risk assessment process is directly related to the impact, criticality and magnitude of the service provider's relationship with CACU.

- Tier 1 service providers are considered critical to the core services provided by CACU, provide services visible to the members and/or have access to member non-public personal information
- Tier 2 service providers are considered important to but are not as critical to CACU's operations
- Tier 3 providers are viewed as non-critical to the daily operations of CACU.

Periodically throughout the term of the contract, each service provider's performance is reviewed and documented appropriately by the service provider relationship owner as determined by the risk assessment. The service provider relationship owner has the following responsibilities:

- Ensuring the completion of a proper due diligence process during the selection and review of service providers
- Ensuring that the appropriate security controls are defined in the contract with the service provider to meet the objectives of Part 748, Appendix A
- Ensuring the appropriate contract legal review is conducted for all service provider relationships
- Monitoring the service provider's performance to contractual commitments and service levels throughout the term of the contract on a continuing basis with annual or more frequent reviews of all obligations identified within the contract.
- Ensuring adequate controls are in place to protect CACU and its members from the risks associated with the service provider relationship
- Completing or updating a risk assessment and determining the proper course of action
- Gathering, reviewing and filing the appropriate due diligence documentation for assigned service providers regularly based on the service provider's classification

Senior management is accountable to the Board of Directors for the review and evaluation of all new and existing service provider relationships. Management and the Board of Directors are responsible for ensuring compliance with CACU's Service Provider Management Policy with respect to significant service provider relationships.

ANNUAL ACH AUDIT CERTIFICATION

As required by the National Automated Clearing House Association (NACHA), CACU has completed its annual audit of the Automated Clearing House (ACH) rules for 2018. This audit was performed in accordance with the requirements set forth in Appendix Eight of the NACHA operating rules by ePayAdvisors, Inc. CACU is pleased to provide our 2018 ACH Appendix Eight Audit Certification for your third party service provider due diligence.

1999 Bryan Street
Suite 950
Dallas, TX 75201
1-800-475-0585 x1601
info@ePayAdvisorrs.com
www.ePayAdvisors.com

January 15, 2018

Corporate America Credit Union
4365 Crescent Road
Irondale, AL 35210

Attn: Lisa Coffey, Chief Operating Officer
Raven Johnson, ACH Leader

2018 ACH Audit Certification

Dear Lisa,

Originating Depository Financial Institutions and Third-Party Service Providers that have agreed with a Participating DFI to process Entries must annually conduct, or have conducted, an audit of its compliance with the Rules in accordance with Appendix Eight (Rule Compliance Audit Requirements).

The ACH Rules Compliance Audit was performed on November 26, 2018 by ePayAdvisors, Inc. for Corporate America Credit Union. The audit performed was not limited to Appendix Eight of the NACHA Operating Rules and was instead expanded to include all Articles and applicable Appendices.

I hereby confirm that Corporate American Credit Union is compliant with Article One, Subsection 1.2.2 of the NACHA Operating Rules.

Sincerely,

Pamela T. Rodriguez

Pamela T. Rodriguez, AAP, CIA, CISA
President & CEO
ePayAdvisors, Inc.
Phone: 800-681-4224 ext. 1107
Fax: 321-280-2530
prodriguez@ePayAdvisors.com
www.ePayAdvisors.com

V 0 6 012018

SSAE 18 STATEMENT

Service Organizational Control #1 (SOC 1) Reports are performed and issued under the Statement on Standards for Attestation Engagements (SSAE) No. 18. The SSAE 18 addresses the importance of accurately disclosing the relationship between the service organization and the subservice organization specifically to identify all subservice organizations used in providing the services and include a description of any subservice organization controls (referred to as Complementary Subservice Organization Controls) that the service organization relies on to provide the primary services to its customers. SSAE 18 also requires a service organization to provide the service auditor with a risk assessment that highlights the organization's key internal risks SSAE 18 also requires a service organization to provide the service auditor with a risk assessment that highlights the organization's key internal risks and monitoring the controls at subservice organizations.

Corporate America has carefully evaluated the costs associated with the preparation of an SSAE 18 audit compared to the extensive compensating controls we currently maintain. It has been determined that at this time, CACU will not engage a firm to perform an SSAE 18 audit.

Corporate America maintains the following risk management infrastructure:

- Complies with the Standards of Professional Practices of Internal Auditing as established by the Institute of Internal Auditors (IIA)
- Employs an internal auditor on staff that reports to our Supervisory Committee
- Supervisory Committee contracts an independent accounting firm to perform annual audits of the corporate's consolidated financial statements, internal controls over financial reporting and general information technology controls
- Contracts third parties with specialized skill sets to conduct audits and/or assessments for internal/external vulnerability assessments, information systems penetration testing, risk assessments and ALM validation testing
- Maintains an extensive Enterprise Risk Management program that includes an independent expert serving on a Board committee
- Staffs positions with professional certifications for accounting (CPA), risk management (CFA), information security (CISSP), ACH (AAP), and auditing (CIA)
- Employs a vendor management program requiring SSAE 18 and/or SOC 1 audit reports from our third party vendors critical to our core services
- Is regulated by the NCUA and Alabama Credit Union Administration (ACUA)

BSA/AML/OFAC

Federal regulatory requirements mandate financial institutions establish and maintain a policy and program to assure and monitor compliance with the requirements of the Bank Secrecy Act (BSA). The Board of Directors at CACU has approved a Regulatory Compliance Policy and Program encompassing BSA, Anti-Money Laundering (AML), Member Identification Program (MIP), and the Office of Foreign Asset Control (OFAC). CACU's Regulatory Compliance program provides a system of controls including but not limited to the following:

- Designated BSA/AML Compliance Officer responsible for oversight and monitoring of compliance
- Review of member accounts in accordance with Section 314(a) of the USA PATRIOT Act
- Member Identification Program (MIP) in accordance with Section 326 of the USA Patriot Act
- Monthly reporting of BSA and OFAC activity to the Board of Directors
- Annual BSA/AML/OFAC Risk Assessment of CACU members, products, and services
- Independent testing (audit)
- Ongoing employee training program

CACU's Regulatory Compliance Program is subject to periodic examination by the NCUA and ACUA.

HUMAN RESOURCES

Background Checks
In compliance with the Fair Credit Reporting Act (FCRA) and applicable state law, a consumer report is obtained for candidates seeking employment or in connection with current employment with CACU after acquiring written authorization. Employment is contingent upon verification of the accuracy of the information obtained during the pre-employment process.

A consumer report includes but is not limited to a complete background check including criminal and credit history, drug screening tests, driving records, school transcripts and any other public information collected in establishing eligibility for employment.

Expectations of Conduct
CACU conducts its business operations in a professional, efficient, ethical, and resourceful manner. The loyalty and the reliable work performance of our employees has been a huge factor in the success of CACU. We expect all employees to conduct themselves with the highest degree of honor, integrity, and character.

Employees must not jeopardize their job duties or responsibilities to CACU, or create a conflict of interest with respect to their obligations to CACU. In particular, employees must conduct themselves so that ethical, legal, or professional questions do not arise with respect to their association with CACU and/or its members.

CACU maintains a Code of Ethics policy which applies to all of our employees, subsidiaries, Board of Directors and Committee members, and contract workers. The values outlined in this policy guide our relationships with members, employees, and the communities we serve.

Confidentiality
CACU employees, subsidiaries, Board of Directors and Committee members, and contract workers understand any information they encounter about CACU or its subsidiaries, member credit unions, or individual members of credit unions while performing their duties is strictly confidential and shall not be discussed or disclosed to anyone outside of CACU. Employees of CACU or its subsidiaries and contract workers are required to sign a confidentiality agreement as a condition of employment.

FIDELITY BOND COVERAGE

NCUA 12 CFR 704.18 states, "All bond forms, and any riders and endorsements which limit the coverage provided by approved bond forms, must receive the prior written approval of NCUA. Fidelity bonds must provide coverage for the fraud and dishonesty of all employees, directors, officers, and supervisory and credit committee members."

CACU maintains a $10 million fidelity bond which is the coverage required by NCUA Part 704.