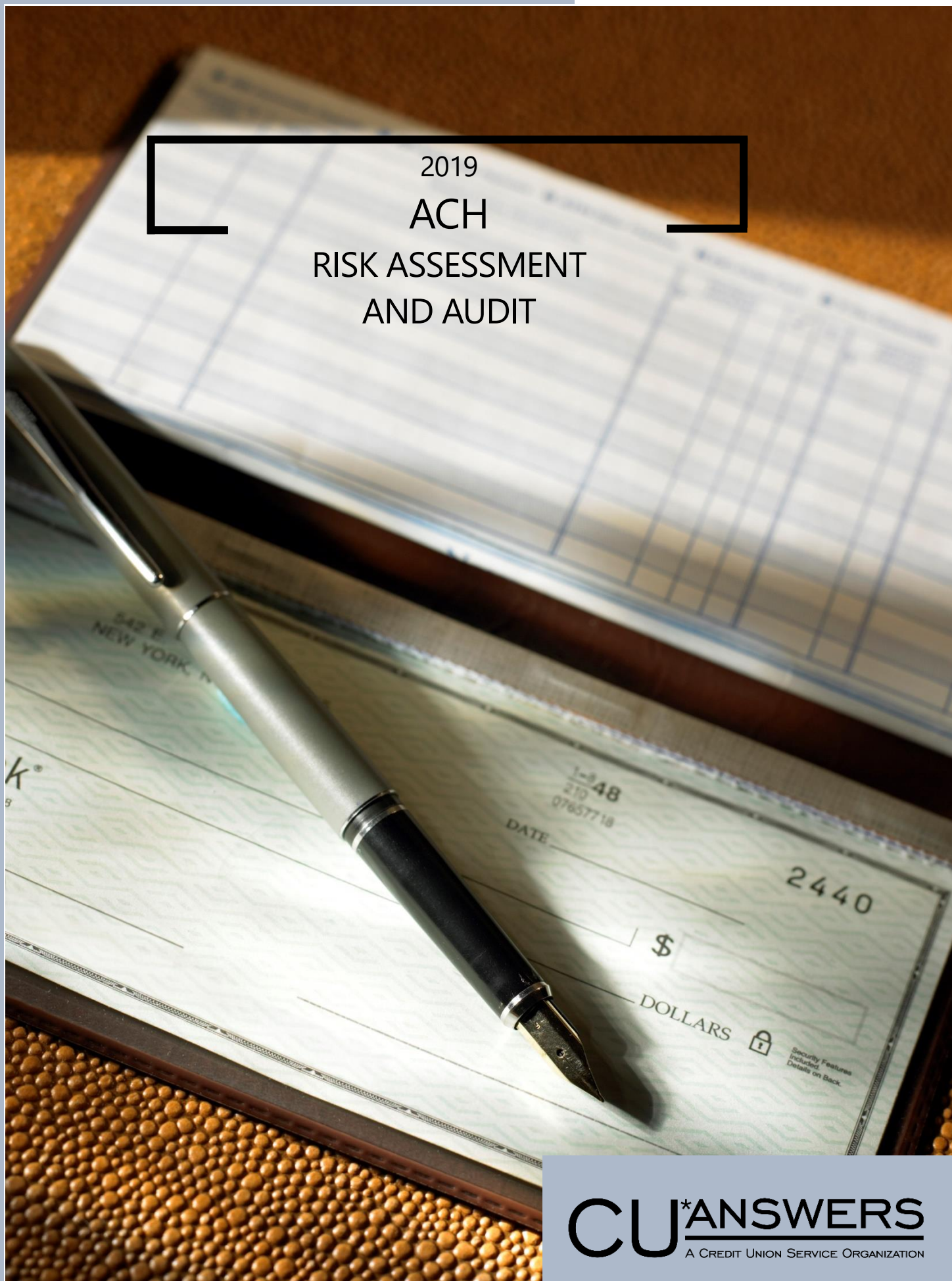
2019

ACH
RISK ASSESSMENT AND AUDIT



CU*ANSWERS
A Credit Union Service Organization

Contents

OVERVIEW

The Board of Directors and Executive Management of The National Automated Clearing House Association ("NACHA") Rule on Section 1, 1.6 requires all Third-Party Service Providers to, as appropriate, update security policies, procedures and systems related to the life cycle of ACH transactions, specifically the initiation, processing and storage of ACH entries.

The core of this risk assessment is as follows:

1. Assessing the nature of risks associated with ACH activity.
2. Performing appropriate due diligence.
3. Having adequate management, information and reporting systems to monitor and mitigate risk.

It is the intent of CU*Answers to understand our risks and include controls that will be evaluated on an annual basis. Our primary risks are transactional and reputational, as well as risks commonly associated with cybersecurity. Policies and processes are designed to mitigate these risks. To assist with managing ACH risk, CU*Answers has qualified staff trained in ACH risk management and NACHA rules. In addition, CU*Answers bi-annually contracts with an external audit firm well-versed in ACH rules to provide an independent evaluation of our ACH compliance.

For the purposes of this report, risk is defined as the probability and frequency of future loss. Methodology for risk determination is accomplished by examining potential threats to operations, weighing the control strength, and determining the severity, if any, of potential losses. Risk of loss is estimated, and therefore not a guarantee of future outcomes.

The estimation of risk in this report is based on industry best practice, financial institution examinational manuals, current risk trends in the industry, and the expertise of the AuditLink team. Executive management and the board of directors generally fulfill their duties under the business judgment rule by being aware of risk within CU*Answers and setting the general risk tolerance of the organization. CU*Answers is not an ACH Originator. Residual risk is partially mitigated through insurance.

Ultimately, risks and results of our ACH audits are made public to our clients, their auditors and examiners, so these entities may independently evaluate our controls and provide reasonable assurance to their management and directors.

Jim Vilker, NCCO, CAMS | CU*Answers | VP Professional Services

Patrick G. Sickels | CU*Answers | Internal Auditor

ACH AUDIT FINDINGS

Originator Obligations

A Third-Party Provider must satisfy NACHA Rule requirements and provide additional warranties for each originated ACH transaction as applicable.

Status of audit requirement: Compliant with Exception

Exception: One Payable file reviewed contained an incorrect Standard Entry Class (SEC) of PPD. The file contained corporate and consumer credit entries. Required Action: To ensure compliance with Nacha Operating Rules, the company must ensure the appropriate SEC code is utilized for consumer (PPD) and corporate (CCD) entries.

Required Action: To ensure compliance with Nacha Operating Rules, the company must ensure the appropriate SEC code is utilized for consumer (PPD) and corporate (CCD) entries.

CU*Answers Response. *CU*Answers has remediated the configuration on its end. CU*Answers is looking for confirmation that its provider (Alloya) has completed its configuration changes.*

ACH DATA FLOWS

DAILY ACH FILES RECEIVED

- CU*Answers receives multiple ACH files throughout the day via FedLine
- Currently, twelve employees are authorized FedLine token holders (Operations)
- Files are delivered and posted to credit union client member accounts on the settlement date. The clients choose the frequency of the postings.
- Clients process their exceptions and returns within CU*BASE GOLD
- A program called "ROBOT" gathers all client returns an authorized employee will send the file via FedLine at 3:00pm

ORIGINATED A2A AND MOP VIA MAGICWRIGHTER

- Clients set member up via the core CU*BASE data processing software to send to a specific account (note that credit union members cannot just set up to any account; the account must be approved by the credit union)
- Member originates the A2A via secure home banking session; the session data is recorded and accessible to the clients via a core log
- Data is collected at CU*Answers level and sent to MagicWrighter via an encrypted "Go Anywhere" session

ACCOUNTING INVOICE ORIGINATION

- CU*Answers uses Great Planes Accounting Software ("GP") and Alloya to process
- Four CU*Answers employees may submit/approve ACH files via Alloya (Accounting)
- The access is only via an individual token which is registered to an individual's desk top computer – the token cannot be used on any other computer or by any other user
- Each employee's Alloya login credentials are tied to the token
- If an employee leaves, the token is returned (as part of company exit interview); the employee is also removed from the account ACH access by a manager)
- Every ACH file submitted requires a two-person process: one employee submits the file, a different employee approves/releases the file
- ACH files are generated via GP; the files are based on the invoices in the system (both accounts receivable and accounts payable) and both of these processes involve verification and approval by those other than the employees entering the data in GP.
- As all client and vendor transactions are entered by staff accountants and reviewed by CFO and/or V.P. of Finance, there is no documented verification of client cards
- Threshold for ACH is $3M (total file size, not individual payments)
- CU*Answers reconciles all bank accounts every month and those reconciliations are reviewed by the CFO
- CU*Answers also has an annual CPA Financial Audit which would uncover any fraudulent activity

ACH RISK ASSESSMENTS

Life Cycle Stage: Data in Transit to and from the Federal Reserve

Governing Policy or Procedures: Operations Run Sheets

INHERENT RISKS	RISK RATING	CONTROLS	RESIDUAL RISKS	RESIDUAL RATING
Data could be exposed to parties not authorized to see it	**HIGH**	*System will not function without encryption*	*The likelihood that our encryption level could be cracked*	**MODERATE (DUE TO HIGH IMPACT OF THE EVENT)**
Communication lines between the Fed and CUA are damaged for an extended period of time	**LOW**	*Tested annually through the DR/BR with complete gap analysis reported to the Board of Directors*	*CU*Answers unable to receive the files in a timely manner*	**LOW**

Life Cycle Stage: Data at Rest

Governing Policy or Procedures: Information Security Program

INHERENT RISKS	RISK RATING	CONTROLS	RESIDUAL RISKS	RESIDUAL RATING
Malicious hacks into our network	**HIGH**	*Firewall maintenance and patch management stays updated and current*	*Theft of information*	**MODERATE (DUE TO HIGH IMPACT OF THE EVENT)**
Malicious hacks into our network	**HIGH**	*External and internal testing of IT controls*	*Theft of information*	**MODERATE (DUE TO HIGH IMPACT OF THE EVENT)**
Internal Employee risk	**HIGH**	*Complete background checks for new hires along with strong system security policies*	*Theft of information*	**MODERATE (DUE TO HIGH IMPACT OF THE EVENT)**
Exposure of materials with sensitive data	**HIGH**	*Policies with audit functionality relating to sensitive data left in the public eye*	*Theft of information*	**MODERATE (DUE TO HIGH IMPACT OF THE EVENT)**

Life Cycle Stage: Data On Backups

Governing Policy or Procedures: Information Security Program

INHERENT RISKS	RISK RATING	CONTROLS	RESIDUAL RISKS	RESIDUAL RATING
Backup media failure	**HIGH**	*System has checks to ensure backup media is functional* *Multiple backup systems in the event of a single system failure*	*Unable to reproduce ACH transactions in the event it would be necessary to repost a file or perform an investigation*	**LOW**
Destruction of the data prior to our retention requirement	**HIGH**	*Records and Information Program*	*Unable to reproduce ACH transactions in the event it would be necessary to repost a file or perform an investigation*	**LOW**
Risk of someone breaking into the facilities or unintended loss while data being transported to the facility	**HIGH**	*Multiple physical controls prevent access to our backup media* *All backups are encrypted* *Encryption key is not on site*	*Theft of the media along with cracking of the encryption or the password keys get stolen*	**LOW**
Unauthorized access to ACH information	**HIGH**	*Library software allows financial institutions to control who can see and access reports*	*Theft of information*	**MODERATE (DUE TO HIGH IMPACT OF THE EVENT)**
Destruction company steals the data	**HIGH**	*Vender management program including legal review of contract, physical site audit, review of insurance and bonding of company*	*Theft of information*	**MODERATE (DUE TO HIGH IMPACT OF THE EVENT)**

Life Cycle Stage: Data in Transit to Client

Governing Policy or Procedures: Operations Run Sheets

INHERENT RISKS	RISK RATING	CONTROLS	RESIDUAL RISKS	RESIDUAL RATING
Same as Federal Reserve	**N/A**	*Same as Federal Reserve*	*Same as Federal Reserve*	**N/A**

CU*ANSWERS	2019
A CREDIT UNION SERVICE ORGANIZATION	

November 6, 2019

Bob Frizzle
CU* Answers
6000 28th Street SE
Grand Rapids, MI 49546

Dear Bob:

Thank you for the hospitality shown to me during my visit at CU* Answers. It was a pleasure visiting with your staff. The external audit of CU* Answers' ACH Operations was performed on September 23-24, 2019 to verify compliance with the ACH Operating Rules. The audit period covered August 12-23, 2019.

Each participating company shall, in accordance with standard auditing procedures, conduct annually an internal or external audit of compliance with the provisions of the ACH rules. Documentation supporting the completion of an audit must be retained for a period of six years from the date of the audit, and provided to the National ACH Association (NACHA) upon request. Additionally, each company shall conduct an assessment of the risks of its ACH activities.

The ACH Audit Management Report is attached herein and intended solely for the information and use of CU* Answers, The Clearing House Payments Authority and the National Automated Clearing House Association. Any suggestions or follow-up items included in the reports should be used for improving operational efficiency, and for maintaining compliance with ACH rules and related regulations.

This audit report does not represent an opinion on the financial condition of CU* Answers. The audit was based on selective sampling of various disclosures and documents pertaining to ACH and a review of compliance with NACHA rules and guidelines and according to industry standards. Conclusions were based on the results of the information reviewed, discussion with various employees and personal observations.

The report is to be used as evidence of performance of the ACH Audit for the calendar year ending December 31, 2019.

Thank you for contracting with The Clearing House Payments Authority to conduct your annual audit.

Sincerely,

The Clearing House Payments Authority

CU*Answers

6000 28th St SE
Grand Rapids, MI 49546

2019 ACH AUDIT MANAGEMENT REPORT

Participants in the ACH network are required to comply with the provisions of the *ACH Operating Rules*. ACH rules provide the requirements for an audit of compliance, and an examination of procedures, policies and controls relating to the origination of ACH entries. Controls include both administrative and operational controls.

CU*Answers is a Third Party Provider of core and peripheral data processing services as a Credit Union Service Organization (CUSO) providing services to client Credit Unions across the United States. CU*Answers core solution, CU*Base, is a software package exclusively owned by CU*Answers. CU*Base services are delivered via online processing, through a data processing center or as an in-house solution. CU*Answers services include receipt and posting of ACH files to the core system and initiate returns on behalf of client Credit Unions. CU*Answers is not a Financial Institution and does not have a routing and transit number.

The ACH Audit of Compliance for CU*Answers was performed on September 23, 2019. The audit period included August 12-23, 2019. Procedures were examined in regard to each applicable requirement with the following results or exceptions.

ACH Audit Requirements

Audits of Rules Compliance
An annual audit must be conducted under these Rule Compliance Audit Requirements no later than December 31 of each year. The Participating DFI, Third-Party Service Provider or Third-Party Sender must retain proof that it has completed an audit of compliance in accordance with these Rules. Documentation supporting the completion of an audit must be (1) retained for period of six years from the date of the audit, and (2) provided to the National Association upon request.

Status of audit requirement: ***Compliant***

Comments: CU*Answers conducted an annual ACH audit of compliance with Nacha Operating Rules for 2013 – 2018; evidence provided. Company obtains ACH audit reports from Magic Wrighter, Alloya Corporate Federal Credit Union, My CU Services LLC (Mid-Atlantic Federal Credit Union), and Payveris.

Electronic Records

A Record required by these rules to be in writing may be created or retained in an electronic form that (a) accurately reflects the information contained within the record, and (b) are capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.

A Record that is required by these Rules to be signed or similarly authenticated may be signed with an Electronic Signature in conformity with the terms of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. §7001, et seq.), and in a manner that evidences the identity of the Person who signed and that Person's assent to the terms of the Record.

Status of audit requirement: ***Compliant***

Comments: Debit and credit entries are posted prior to open of business, intraday as received and at end of day processing; evidence of credit funds availability provided. CU*Answers, by agreement, provides electronic records to its clients for purpose of audit trail to ensure compliance with Nacha Operating Rules and regulatory requirements. Clients can opt to receive 90 days of electronic records by disk for retention purposes. Some clients opt to retain daily reports/files within their own internal imaging system.

CU*Answers provides client Credit Unions with OFAC SDN review of received International ACH Transactions (IAT); evidence of provided. Company indicates all appropriate lines of addenda are reviewed. Client Credit Unions are responsible for additional review and posting of suspect entries.

CU*Answers extracts client return and NOCs for transmission to the Federal Reserve Bank as ACH Operator; evidence of retention provided for 2013 through current date 2019.

CU*Answers provides statement services to client Credit Unions; appropriate transaction information passes to the account statement.

Security of Protected Information

Each Non-consumer Originator, Participating DFI, and Third-Party Service Provider must establish, implement, and update, as appropriate, policies, procedures, and systems with respect to the initiation, processing, and storage of Entries that are designed to (a) protect the confidentiality and integrity of Protected Information until its destruction; (b) protect against anticipated threats or hazards to the security or integrity of Protected Information until its destruction; and (c) protect against unauthorized use of Protected Information that could result in substantial harm to a natural person. Such policies, procedures, and systems must include controls that comply with applicable regulatory guidelines on access to all systems used by such Non-Consumer Originator, Participating DFI, and Third-Party Service Provider to initiate, process, and store Entries.

The ACH security requirements consist of three elements (1) the protection of sensitive data and access controls; (2) self-assessment; and (3) verification of the identity of Third-Party Senders and Originators.

Status of audit requirement: ***Compliant***

Comments: CU*Answers conducts an annual ACH Risk Assessment that includes the data of security of protected information. All assessments and audits are presented to the Board of Directors upon completion.

Company provided evidence of the CU*Answers 2017 SOC 1 Type 2, the 2018 SOC 2 Type 2, and the CU*Base and Network Services SOC 1 Type 2.

Company obtains evidence of risk assessment reports from Magic Wrighter, Alloya Corporate Federal Credit Union, My CU Services LLC (Mid-Atlantic Federal Credit Union), and Payveris.

Physical and logical access to the building and systems is secure and review of access rights every 92 days and as employees are hired or termination. Continual and ongoing basis for access to Fedline, etc. (Review SOC)

Encryption

Banking information related to an Entry that is Transmitted via an Unsecured Electronic Network must, at all times from the point of data entry and through the Transmission of such banking information, be either encrypted or Transmitted via a secure session, in either case using a technology that provides a commercially reasonable level of security that complies with applicable regulatory requirements.

Status of audit requirement: ***Compliant***

Comments: Evidence of encryption was provided for online banking provided by CU*Answers, the Membership Opening Product (MOP) and A2A (funding for both services provided by Magic Wrighter), and P2P (provided by Payveris).

CU*Base client connectivity is by secure VPN or dedicated Multiprotocal Label Switching (MPLS) with VPN back-up.

Agreements

When agreements have been executed between the Originator and the ODFI, it is also recommended that agreements be entered into between the Originator and the Third-Party Service Provider, and between the Third-Party Service Provider and the ODFI.

Status of audit requirement: ***Compliant***

Comments: CU*Answers executes a Master Services Agreement with its client Credit Unions; evidence of agreements provided for selected clients. *Schedule B – ACH Operator Services* of each agreement identifies ACH activity roles and responsibilities of the client and CU*Answers. Agreements may be signed physically or by electronic method. All agreements are scanned into *The Corporate Vault*, an internally hosted image system. Access is restricted to the Accounting Department.

Return Entries

A Third-Party Provider must accept Return Entries and Extended Return Entries received from an RDFI. Dishonored Return Entries must be transmitted within five Banking Days after the Settlement Date of the Return Entry and contested dishonored Return Entries must be accepted, as required by these Rules.

A Third-Party Provider may Reinitiate an Entry, other than an RCK Entry, that was previously returned as established in these Rules. A Third-Party Provider may originate a Return Fee Entry to the extent permitted by applicable Legal Requirements and as established in these Rules.

Status of audit requirement: ***Not Applicable***

Comments: CU*Answers does not process stop payments or unauthorized returns, or make pay/return decisions on behalf of client credit unions; each credit union is responsible for working its exceptions/.

Notification of Change

An ODFI must accept a Notification of Change ("NOC" and "COR Entry") or a corrected NOC and provide Originator with notification as identified in these Rules. An Originator must make the changes specified

in the NOC or corrected NOC within six Banking Days of receipt of the NOC information or prior to initiating another Entry to a Receiver's account, whichever is later.

Status of audit requirement: ***Not Applicable***

Comments: CU*Answers does not create Notifications of Change (NOC) on behalf of client Credit Unions; each Credit Union is responsible for working its exceptions.

Request for Authorization

An authorization must be obtained from a Receiver to originate one or more Entries to the Receivers account; and at the request of the ODFI, the Third-Party or Originator must provide a copy of such authorizations in accordance with the requirements of these rules.

Status of audit requirement: ***Compliant***

Comments: Debit authorization agreements are contained within the client agreements.

Reversing Entries and Reversing Files

A Third-Party Provider may initiate a Reversing File to reverse all Entries of an Erroneous File or a Reversing Entry to correct an Erroneous Entry previously initiated to a Receivers account in accordance with the requirements of the Rules.

Status of audit requirement: ***Not Applicable***

Comments: CU*Answers does not originate ACH transactions on behalf of its Credit Union clients; reversing entries and files is not applicable.

Originator Obligations

A Third-Party Provider must satisfy NACHA Rule requirements and provide additional warranties for each originated ACH transaction as applicable.

Status of audit requirement: ***Compliant with Exception***

CU*Answers does not originate ACH transactions on behalf of its Credit Union clients. Company utilizes Magic Wrighter for funding of Account to Account (A2A) transactions. The client credit unions are identifies as the Originating Depository Financial Institution (ODFI); clients contract directly with Magic Wrighter. CU*Answers utilizes Payveris for Person to Person (P2P) transactions, Webster Bank is identified as the ODFI.

PPD (Prearranged
CCD (Corporate Credit or Debit Entry)
CTX (Corporate Trade Exchange Entry)
Compliance with formatting and authorization requirements.

Comments:

CU*Answers utilizes Microsoft Dynamics GP (Great Plains) accounting software for monthly collection of payment from client Credit Unions and vendor payments via ACH. Files are originated through Alloya and subject to dual control.

ACH files for collection of payment from client Credit Unions appropriately identified CU*Answers in the Company Name field and contained the appropriate SEC code CCD.

Exception: One Payable file reviewed contained an incorrect Standard Entry Class (SEC) of PPD. The file contained corporate and consumer credit entries.

Required Action: To ensure compliance with Nacha Operating Rules, the company must ensure the appropriate SEC code is utilized for consumer (PPD) and corporate (CCD) entries.

This audit was conducted at the office of CU*Answers, 4695 44th St SE (Building B), Kentwood, MI in compliance with the *ACH Operating Rules, Article Two and all other applicable Appendixes.*

Christina Poole, AAP, APRP, CUCE
Professional Services - Audit
The Clearing House Payments Authority
580 Kirts Boulevard
Troy, MI 48084

Submitted for Review: Lisa Iselli, AAP, APRP November 3, 2019

2019 ACH Audit Certification

Company Name: **CU*Answers**

Date of Audit: **September 23, 2019**

Audit Period: **August 12-23, 2019**

Auditor Name: **Christina Poole, AAP, APRP, CUCE**

The ACH annual audit was completed in compliance with *ACH Operating Rules* by The Clearing House Payments Authority, a NACHA Direct Member.

The Clearing House Payments Co., LLC
1114 Avenue of the Americas, 17th Floor
New York, NY 10036

NACHA DIRECT MEMBER
Regional Payments Association®

"The Mark of Excellence"
This mark signifies that the Regional Payments Associations, through their Direct Membership in NACHA, are specially recognized and licensed providers of ACH education, publications and support. Regional Payments Associations are directly engaged in the NACHA Rulemaking Process and Accredited ACH Professional (AAP) program. Look for this mark as a sign of excellence and commitment to consistency and accuracy in ACH education, publications and support.