AuditLink

2021
Annual ACH Risk Assessment and Data Security Self-Assessment
CU*Answers

July 1, 2021

Jim Vilker, NCCO, CAMS
VP Professional Services
6000 28th St SE
Grand Rapids, MI
800-327-3478 ext.167

CU*ANSWERS Management Services

LEGAL DISCLAIMER

The information contained in this document does not constitute legal advice. We make no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained in this document. You should retain and rely on your own legal counsel, and nothing herein should be considered a substitute for the advice of competent legal counsel. These materials are intended, but not promised or guaranteed, to be current, complete, and up-to-date and should in no way be taken as an indication of future results. All information is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will CU*Answers, its related partnerships or corporations, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information provided or for any consequential, special or similar damages, even if advised of the possibility of such damages.

July 1, 2021
CU*Answers
AuditLink
6000 28th Street SE
Grand Rapids, MI 49546

Letter to Clients

The Board of Directors and Executive Management of The National Automated Clearing House Association ("NACHA"), Rule 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:

Assessing the nature of risks associated with ACH activity.	**Performing appropriate due diligence.**	**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 Data Flows

DAILY ACH FILES RECEIVED VIA CU*BASE

01 FedLine
CU*Answers receives multiple ACH files throughout the day via FedLine

02 Security Token
As of July 1, 2021, ten employees are authorized FedLine token holders (Operations Team)

03 File Posting
Files are delivered and posted to credit union client member accounts on the settlement date; credit union clients choose the frequency of the postings

04 Exception processing
Clients process their exceptions and returns within CU*BASE GOLD

05 Client Returns
A program called "ROBOT" gathers all client returns while an authorized employee will send the file via FedLine at 3:00pm

ORIGINATED A2A AND MOP VIA MAGICWRIGHTER

01 Credit Union Setup
Credit union clients set members 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)

02 Online Banking
Member originates the A2A via secure home banking session; the session data is recorded and accessible to the clients via a core log

03 MagicWrighter
Data is collected at CU*Answers level and sent to MagicWrighter via an encrypted "Go Anywhere" session

CU*ANSWERS ACCOUNTING INVOICES

CU*Answers uses Great Plains Accounting Software ("GP") and Alloya to process

01 Credit Union Setup
As of July 1, 2021, four CU*Answers employees may submit/approve ACH files via Alloya (Accounting)

02 Security Token
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

03 Credentials
Each employee's Alloya login credentials are tied to the token

04 Access Removal
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)

05 File Submission
Every ACH file submitted requires a two-person process: one employee submits the file; a different employee approves/releases the file

06 File Generation
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

07 Executive Review
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

08 File Limit
Threshold for ACH is $3M (total file size, not individual payments)

09 Reconcilliation
CU*Answers reconciles all bank accounts every month and those reconciliations are reviewed by the CFO

10 Annual Audit
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**	Firewall maintenance and patch management stays updated and current	The likelihood that our encryption level could be cracked	**MODERATE (DUE TO HIGH IMPACT OF THE EVENT)**
*Communication lines between the Fed and CU*Answers are damaged for an extended period*	**LOW**	Tested through the DR/BR with 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**	Vendor 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**

2020 ACH Audit Findings Response

No findings.

The Clearing House®

September 7, 2021

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

Dear Bob:

Thank you for contracting with The Clearing House Payments Authority for your ACH Audit. It was a pleasure working with your staff. The external audit of CU*Answers, Inc.'s ACH Operations was performed on July 13-14, 2021 to verify compliance with the ACH Operating Rules. The audit sample period covered Ma 17-28, 2021.

Each participating organization 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 organization 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, Inc., The Clearing House Payments Authority and the National Automated Clearing House Association. Any suggestions or follow-up items included in the report 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, Inc. 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.

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

ACH Audit Summary 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 Service 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 July 13-14, 2021. The audit sample period included May 17-28, 2021. Procedures were examined in regard to each applicable requirement with the following results:

Audits of Rules Compliance	**Compliant**
Electronic Records	**Compliant**
Security of Protected Information	**Compliant**
Encryption	**Compliant**
Agreements	**Compliant**
Return Entries	**Compliant**
Notifications of Change	**Compliant**
Request for Authorization	**Compliant**
Reversing Entries and Reversing Files	**Not Applicable**
Originator Obligations	**Compliant**

This audit was conducted for CU*Answers in compliance with the *ACH Operating Rules, Article Two and all other applicable Appendixes.*

Christina Poole, AAP, APRP, CUCE
Payments Consulting & Compliance
The Clearing House Payments Authority
580 Kirts Boulevard
Troy, MI 48084

Reviewed By: Adrian Brown, AAP, APRP, September 2, 2021

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: ***Compliant***

Comments: CU*Answers conducted an ACH Audit for 2020; evidence of retention of 2016-2019 audits was available for review. An attestation of completion of the most recent ACH audit was obtained for applicable Third-Party Providers of ACH services.

All assessment and audit reports conducted for or by CU*Answers are presented to the Board of Directors upon completion and made available to clients through the company website.

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: ***Compliant***

Comments: Received Entries are posted and funds made available as required. Evidence of Same Day ACH funds availability provided for all applicable time-frames.

By agreement, CU*Answers provides electronic records to its clients for evidence of compliance with Nacha Operating Rules and regulatory requirements. Clients receive 90 days of electronic records and may opt to retain daily reports within their own internal servers.

CU*Answers conducts OFAC SDN review of its clients received International ACH Transactions (IAT). Company indicates all appropriate lines of addenda are reviewed; additional review of suspect transactions are the responsibility of clients.

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.

Effective June 30, 2021: *Each Non-Consumer Originator that is not a Participating DFI, each Third-Party Service Provider, and each Third-Party Sender, whose origination or transmission volume exceeds 6 million entries annually must, by June 30 of the following year, protect DFI account numbers used in the initiation of Entries by rendering them unreadable when stored electronically.*

Status: ***Compliant***

Comments: CU*Answers completed an ACH Risk Assessment and Data Security Self-Assessment in July 2021. The security of protected information is identified in company policies.

CU*Answers completes annual due diligence on all vendors including a Critical Vendor Risk Assessment. Evidence of risk and security assessments is obtained from applicable Third-Party Service Providers of ACH services.

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: ***Compliant***

Comments: CU*Answers provides online banking for its clients; evidence of encryption provided. The option for person to person transactions (P2P) and bill payment services is provided by Payveris. Additional services provided include Membership Opening Product (MOP) and A2A; funding for both services provided by Magic Wrighter.

CU*Base client connectivity is by dedicated secure VPN or dedicated Multiprotocol 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.

Such agreements should acknowledge that Entries may not be initiated the violate the laws of the United States; that includes any restrictions on types of Entries that may be originated; that include the right to terminate or suspend the agreement for breach of the Rules, and the right to audit.

Status: ***Compliant***

Comments: CU*Answers provides services to approximately 200 Credit Unions nationally. A Master Services Agreement is executed with each client Credit Union; evidence of agreements provided for selected clients.

Return Entries

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

Status: ***Compliant***

Comments: CU*Answers does not process returns or make pay/return decisions on behalf of client Credit Unions; each client is responsible for working its exceptions. Upon receipt of client return files, CU*Answers transmits files to the Federal Reserve as ACH Operator.

Notification of Change

A Third-Party Service Provider 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: ***Compliant***

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. Upon receipt of client NOC files, CU*Answers transmits files to the Federal Reserve as ACH Operator.

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: ***Compliant***

Comments: Debit authorization agreements are contained within the client agreements; evidence provided.

Reversing Entries and Reversing Files

A Third-Party Service 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: ***Not Applicable***

Comments: CU*Answers does not originate ACH transactions on behalf of its Credit Union clients; reversing entries and files is not applicable. There have been no instances in which a client debit file would need to be reversed.

Originator Obligations

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

Status: ***Compliant***

CU*Answers does not originate ACH transactions on behalf of its Credit Union clients. Company offers origination services through Magic Wrighter; client Credit Unions contract directly with Magic Writher and are identified as the Originating Depository Financial Institution (ODFI). CU*Answers offers additional online banking services (bill payment, A2A/P2P) through Payveris and its ODFI.

PPD (Prearranged Payment and Deposit Entry)
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 to initiate vendor payments via ACH. Files are originated through Alloya and require to dual control.

ACH files for collection of payment from client Credit Unions identify CU*Answers in the Company Name field and contain the appropriate Standard Entry Class (SEC) code CCD.

ACH Audit Certification

Company Name:	CU*Answers
Date of Audit:	July 13-14, 2021
Audit Sample Period:	May 17-28, 2021
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