

2024 Annual ACH Risk Assessment

July 8, 2024

CU*ANSWERS, A CREDIT UNION SERVICE ORGANIZATION



6000 28th Street SE
Grand Rapids, MI 49546
800.327.3478
www.cuanswers.com

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, or 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.

Letter to Clients

July 8, 2024

CU*Answers, A Credit Union Service Organization
6000 28th Street SE
Grand Rapids, MI 49546

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 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.

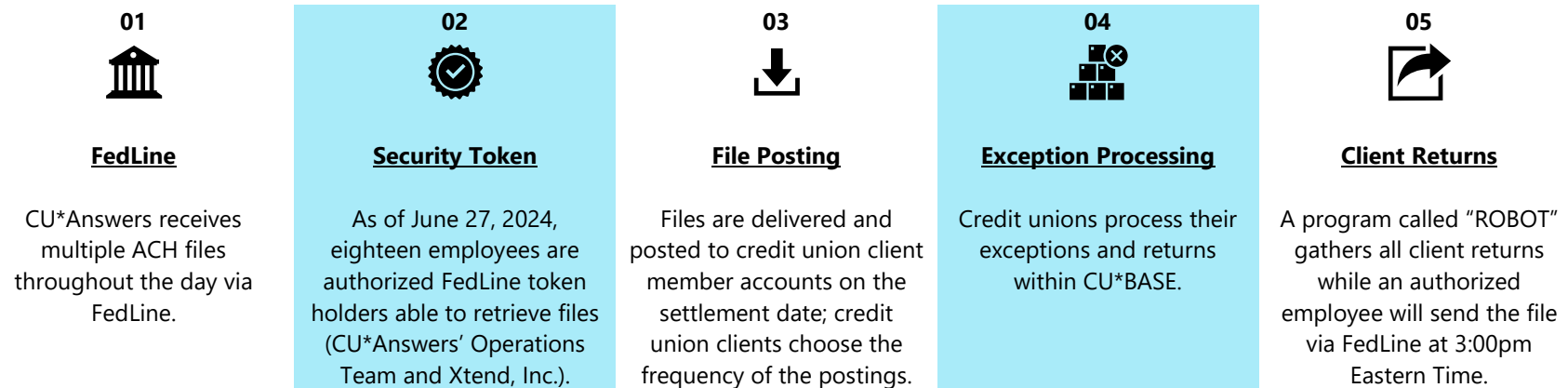
The estimation of risk in this report is based on industry best practice, financial institution examination manuals, current risk trends in the industry, and the expertise of the CU*Answers staff. Executive management and the board of directors generally fulfill their duties under the business judgment 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.

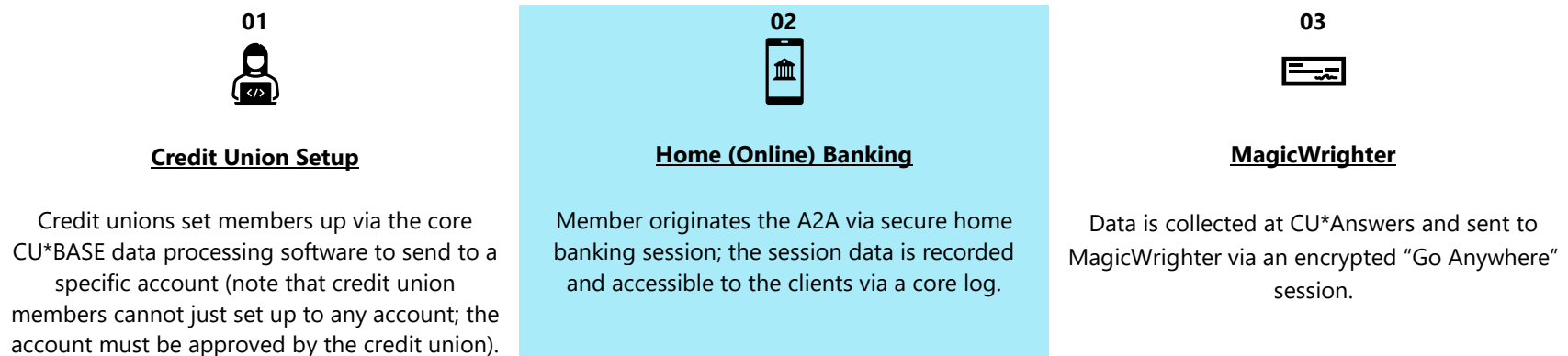
Patrick G. Sickels
General Counsel and Director of Internal Audit
CU*Answers, A Credit Union Service Organization

Description of ACH Data Flows

Daily ACH Files Received via CU*BASE



Originated A2A and MOP via MagicWrighter



CU*Answers Accounting Invoices

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

01



Authorization

As of June 26, 2024, five 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 desktop 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 VP of Finance/Accounting Manager; there is no documented verification of client cards.

08



File Limit

Threshold for ACH is \$4M (total file size, not individual payments).

09



Reconciliation

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

ASSET	REASONABLY FORESEEABLE THREATS	THREAT DESCRIPTION	LIKELIHOOD	IMPACT	CONTROLS	LIKELIHOOD WITH CONTROLS	RESIDUAL RISK	RISK REVIEW
ACH Data Files	<p>Mishandling of critical and/or sensitive information by employees.</p> <p>Exploit poorly configured or unauthorized information systems exposed to the Internet.</p>	Unauthorized access either due to inadvertent exposure or malicious attackers.	MODERATE	VERY HIGH	<p>Run Sheets* Operators have instructions and record all events in run sheets.</p> <p>Firewall Maintenance and Vulnerability Management* Firewall maintenance and patch management stays updated and current.</p> <p><i>*See the most recent SSAE-18 SOC report (or equivalent) for additional details.</i></p> <p>Encryption ACH Files are encrypted with industry standard encryption in transit and at rest.</p> <p>FedLine Access FedLine access is limited to authorized employees. Background checks are performed for all new hires.</p>	LOW	MODERATE* <i>*Due to the high impact of a potential event.</i>	Annual
ACH Data Files	Unable to transmit or receive ACH files.	Communication lines between the Fed and CU*Answers are damaged for an extended period.	LOW	VERY HIGH	<p>Business Continuity Testing Tested at least twice annually with gap analysis reported to the Board of Directors and to all clients (available on CU*Answers' website).</p>	VERY LOW	LOW	Annual (with Business Continuity plans updated at least twice annually).

Life Cycle Stage: Data at Rest
Governing Policy or Procedures: Information Security Program

ASSET	REASONABLY FORESEEABLE THREATS	THREAT DESCRIPTION	LIKELIHOOD	IMPACT	CONTROLS	LIKLELIHOOD WITH CONTROLS	RESIDUAL RISK	RISK REVIEW
ACH Data Files	<p>Mishandling of critical and/or sensitive information by employees.</p> <p>Exploit poorly configured or unauthorized information systems exposed to the Internet.</p>	Unauthorized access either due to inadvertent exposure or malicious attackers.	MODERATE	VERY HIGH	<p>Firewall Maintenance and Vulnerability Management* Firewall maintenance and patch management stays updated and current.</p> <p>External and Internal Testing of IT Controls* Controls are tested regularly, with external testing performed on no less than an annual basis.</p> <p>Library Segregation* The data processing software allows financial institutions to control who can see and access reports.</p> <p><i>*See the most recent SSAE-18 SOC report (or equivalent) for additional details.</i></p> <p>Encryption ACH Files are encrypted with industry standard encryption in transit and at rest.</p> <p>FedLine Access FedLine access is limited to authorized employees. Background checks are performed for all new hires.</p>	VERY LOW	MODERATE* <i>*Due to the high impact of a potential event.</i>	Annual

Life Cycle Stage: Data on Backups
Governing Policy or Procedures: Information Security Program

ASSET	REASONABLY FORESEEABLE THREATS	THREAT DESCRIPTION	LIKELIHOOD	IMPACT	CONTROLS	LIKELIHOOD WITH CONTROLS	RESIDUAL RISK	RISK REVIEW
ACH Data Files	Unauthorized access to data.	Unauthorized access either due to inadvertent exposure or malicious attackers.	LOW	VERY HIGH	<p>Encryption ACH Files are encrypted with industry standard encryption and the encryption key is not stored on-site.</p> <p>Physical Access* Multiple physical controls prevent access to our backup media.</p> <p>Library Segregation* The data processing software allows financial institutions to control who can see and access reports.</p> <p><i>*See the most recent SSAE-18 SOC report (or equivalent) for additional details.</i></p> <p>Destruction Vendor Review CU*Answers has a vendor management program including legal review of contract, physical site audit, review of insurance and bonding of company</p>	VERY LOW	MODERATE* <i>*Due to the high impact of a potential event.</i>	Annual

Life Cycle Stage: Data on Backups (continued)
Governing Policy or Procedures: Information Security Program

ASSET	REASONABLY FORESEEABLE THREATS	THREAT DESCRIPTION	LIKELIHOOD	IMPACT	CONTROLS	LIKELIHOOD WITH CONTROLS	RESIDUAL RISK	RISK REVIEW
ACH Data Files	Loss of data on backups.	Data is either improperly backed up, media fails, or data is destroyed inadvertently.	LOW	VERY HIGH	<p>Backup Media Checks The system has checks to ensure correct data is transmitted to backup media and the media is functional. In many cases, CU*Answers can also reproduce ACH transactions in the event it would be necessary to repost a file or perform an investigation.</p> <p>Failover Systems Multiple backup systems exist in the event of a single system failure.</p> <p>Retention CU*Answers has a Records and Information (RIM) program to assist with the prevention of destruction of data prior to the retention expiration.</p>	VERY LOW	LOW	Annual

Life Cycle Stage: Data in Transit to Client
Governing Policy or Procedures: Operations Run Sheets

ASSET	REASONABLY FORESEEABLE THREATS	THREAT DESCRIPTION	LIKELIHOOD	IMPACT	CONTROLS	LIKELIHOOD WITH CONTROLS	RESIDUAL RISK	RISK REVIEW
ACH Data Files	CU*Answers does not have risks independent from the Federal Reserve.	n/a	N/A	N/A	CU*Answers does not have controls independent from the Federal Reserve.	N/A	N/A	n/a



September 24, 2024

Geoff Johnson
CU*Answers, Inc.
6000 28th Street SE
Grand Rapids, MI 49546

Dear Geoff:

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 activity was performed on August 16, 2024, to verify compliance with the ACH Operating Rules. The audit sample period covered May 6 – 17, 2024.

Each participating Third-Party Sender 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 Third-Party Sender 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, Inc.

6000 28th Street SE
Grand Rapids MI 49546

ACH AUDIT MANAGEMENT REPORT SUMMARY

Participants in the ACH network are required to comply with the provisions of the *Nacha Operating Rules*. The Rules require any Third-Party Service Provider or Third-Party Sender that performs a function of ACH processing conduct an annual audit of compliance with the requirements of the *Nacha Operating Rules* as applicable to the services provided. In addition to an audit of compliance, the Rules provide guidance for an examination of operational controls, policies, and procedures relating to the origination of ACH entries.

CU*Answers is acting as a Third-Party Service Provider (TPSP) of core and peripheral data processing services as a Credit Union Service Organization (CUSO). They provide 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 systems 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 August 16, 2024. The audit sample period included May 6 – 17, 2024. Procedures were examined in regard to each applicable requirement with the following results or exceptions.

Audits of Rules Compliance	Compliant
Risk Assessment	Compliant
Electronic Records and Electronic Signatures	Compliant
Security of Protected Information	Compliant
Secure Transmission of ACH Information	Compliant
Agreements	Compliant
Return Entries	Compliant
Notifications of Change	Compliant
Reversing Files and Reversing Entries	Not Applicable
Origination Obligations	Compliant

This audit was conducted for CU*Answers, in compliance with the ACH Operating Rules, Article Two and all other applicable Appendixes. Any comments and recommendations should be used for improving operational efficiency, and for maintaining compliance with ACH rules and related regulations.

Joe Allen, AAP
Payments Compliance
The Clearing House Payments Authority

Reviewed By: Christina Rice, AAP, APRP, NCP
September 6, 2024

ACH Audit Requirements

Audits of Rules Compliance

A Participating DFI must annually conduct, or have conducted, an audit of its compliance with these Rules. A Third-Party Service Provider or Third-Party Sender that has agreed with a Participating DFI to process Entries must annually conduct, or have conducted, an audit of its compliance with these Rules. 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 retained for a period of six years from the date of the audit. Upon receipt of the National Association's request, a Participating DFI must provide to the National Association, within ten (10) Banking Days, proof that the Participating DFI and/or any requested Third-Party Service Provider(s) or Third-Party Sender(s) have completed audits of compliance in accordance with these Rules.

Status: ***Compliant***

Comments: CU*Answers conducts an annual ACH audit and were provided for review for 2018-2023. ACH Risk Assessments were also provided for review. CU*Answers, as part of its Vendor Management program, obtains the ACH audits for its applicable vendors. The Board is informed of all audit findings and tracking has been implemented for audit finding remediation purposes.

In order to facilitate the Credit Unions that CU*Answers serves, a due diligence portal was created; site is utilized to provide easy access to ACH audits and SOC reports, upon request, to the Financial Institutions.

Credit Unions are trained and provided procedures and processes for ACH file processing.

Risk Assessment

A Participating DFI and a Third-Party Sender must (a) conduct, or have conducted, an assessment of the risks of its ACH activities; (b) implement or have implemented, a risk management program on the basis of such an assessment; and (c) comply with the requirements of its regulator(s) with respect to such assessment and risk management program.

Status: ***Compliant***

Comments: CU*Answers conducted an ACH Risk Assessment in 2024; controls, policies, and procedures are all in place to assist in the management of risk within the organization. CU*Answers partners with a third-party vendor to conduct an annual SOC report for review of risk and other factors within the organization; completion of last report was in July of 2024.

Electronic Records and Electronic Signatures

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: CU*Answers maintains electronic records of all transactions for evidence of compliance with Nacha Operating Rules. Per Staff, all records are maintained and protected for a minimum of seven years.

Security of Protected Information

Each Non-consumer Originator, Participating DFI, Third-Party Service Provider, and Third-Party Sender 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.

Each Non-Consumer Originator that is not a Participating DFI, each Third-Party Service Provider, and each Third-Party Sender, whose ACH origination or transmission volume exceeds 2 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 maintains Cyber Security, Information Security, and Physical Security policies. Data security, storage, and destruction are identified within the policies. CU*Answers partners with a third-party vendor to conduct annual SOC reports; data security is included within the report. Documentation was provided in the portal for review.

Secure Transmission of ACH Information via Unsecured Electronic Networks

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 maintains Cyber Security, Information Security, and Physical Security policies; encryption standards are identified within the policies. Evidence of encryption for all platforms, internal and through external vendors, was provided for review.

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. The executed agreement between and ODFI and Third-Party Service Provider may be based on the facts and circumstances of the business arrangement. This agreement should define the responsibility, accountability, and liability for the handling of ACH files. The agreement should address responsibilities of each party regarding quality of data, input schedules and deadlines, and any other issues pertinent to the actual processing and delivery of the payment data.

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

Status: **Compliant**

Comments: CU*Answers provides ACH services for approximately 200 Credit Unions. Proof of Executed Master Services Agreement was provided for selected Credit Unions. Agreements stored electronically.

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: All return entries are received and passed directly to the Credit Unions utilizing CU*Answers core software; each Credit Union is responsible for the working of their own returns and exceptions. CU*Answers does not manually work return entries for its clients.

Notification of Change

A Third-Party Service Provider must accept a Notification of Change (“NOC” and “COR Entry”) or a corrected NOC and provide the Originator or Third-Party Sender with notification as identified in these Rules. An Originator or Third-Party Sender 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: Notifications of Change (NOC) are received by CU*Answers and passed directly to the Credit Unions; each Credit Union is responsible for working its NOCs and exceptions. The Credit Union will then transmit the NOC back to CU*Answers for distribution to the ACH Network. CU*Answers does not manually work NOC entries for its clients.

Reversing Files and Reversing Entries

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 entries into the network for its clients and therefore will not initiate Reversal entries.

Origination Obligations

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

Status: **Compliant**

Comments: CU*Answers utilizes Microsoft Great Plains software for collections of CUSO payments. Alloya Federal Credit Union is utilized for the entries. CU*Answers is not the ODFI for the entries. Attestation to Alloya's ACH audit was provided for review.



ACH Audit Certification

Company Name: CU*Answers, Inc.
Date of Audit: August 15 – 16, 2024
Audit Sample Period: May 6 – 17, 2024
Auditor Name: Joe Allen, AAP

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

