# 2025

# Annual ACH Audit and Risk Assessment

On an annual basis, the CU*Answers Board of Directors causes an ACH Audit and an ACH Risk Assessment to be performed, for the purpose of assisting all clients with due diligence requirements.

## VIST US ON THE WEB

For additional due diligence information, including SOC reports and financial statements, visit us at:
**https://www.cuanswers.com/about/due-diligence-materials/**

**LEGAL DISCLAIMER**

**6000 28TH STREET S.E. • GRAND RAPIDS, MI 49546**
phone: 616.285.5711 • 800.327.3478 • fax: 616.285.5735
visit us on the web: www.cuanswers.com

## Letter to Clients

August 14, 2025

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, the risks and results of our ACH audits are made public to our clients, and to 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/CBX

| 01 FedLine | 02 Security Token | 03 File Posting | 04 Exception Processing | 05 Client Returns |
|---|---|---|---|---|
| CU*Answers receives multiple ACH files throughout the day via FedLine. | Designated employees are authorized FedLine token holders to retrieve files. | Files are delivered and posted to credit union client member accounts on the settlement date; credit union clients choose the frequency of the postings. | Credit unions process their exceptions and returns within CU*BASE. | A program called "ROBOT" gathers all client returns while an authorized employee will send the file via FedLine at 4:00pm Eastern Time. |

## Originated A2A and MOP via Payment Processor

| 01 Credit Union Setup | 02 Home (Online) Banking | 03 Payment Processor |
|---|---|---|
| Credit unions set members up via the core CU*BASE/CBX 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 and sent to the payment processor via an encrypted "Go Anywhere" session. |

# CU*Answers Accounting Invoices

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

**01**
**Authorization**

Designated CU*Answers Accounting Team employees may submit and/or approve ACH files via Alloya.

**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. Each employee's Alloya login credentials are tied to the token.

**03**
**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. Threshold for ACH is $4M (total file size, not individual payments).

**04**
**File Submission**

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

**05**
**File Generation**

ACH files are generated via GP; the files are based on the invoices in the system (both accounts receivable and accounts payable). Both processes involve verification and approval by other employees.

**06**
**Executive Review**

As all client and vendor transactions are entered by staff accountants and reviewed by management.

**07**
**Reconciliation**

CU*Answers reconciles all bank accounts every month and those reconciliations are reviewed by the Accounting Team.

**08**
**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: Information Security Program*

| THREAT | INITIAL THREAT/RISK SCORING | | CONTROLS/MITIGATION MEASURES | CONTROLS EFFECTIVENESS | RESIDUAL RISK SCORE |
|---|---|---|---|---|---|
| **SECURITY THREATS** | | | | | |
| Physical Theft of Hardware | Probability | 2 | Physical access controls; restricted access to data centers; background checks on employees | Moderately Effective | **Medium** |
| | Severity | E | **Medium** | | |
| Improper Handling of Sensitive Information | Probability | 2 | Technical controls on electronic data, including encryption and access by job role | Moderately Effective | **Medium** |
| | Severity | D | **Medium** | | |
| Social Engineering | Probability | 5 | Awareness training, firewall controls, web filters | Mostly Effective | **Medium** |
| | Severity | E | **Very High** | | |
| Unauthorized External Access | Probability | 2 | Firewall, whitelisting, vulnerability management and intrusion detection | Mostly Effective | **Medium** |
| | Severity | E | **Medium** | | |
| Unauthorized Internal Access | Probability | 2 | Least privilege access; limited FedLine access; application login and menu controls; background checks on employees | Mostly Effective | **Medium** |
| | Severity | D | **Medium** | | |
| Falsified Input | Probability | 2 | Application login controls, including limitations of access and individualized logins | Moderately Effective | **Very Low** |
| | Severity | B | **Very Low** | | |
| Negligence or Human Error | Probability | 1 | Run sheet review; automated ROBOT processing | Mostly Effective | **Low** |
| | Severity | D | **Very Low** | | |
| Unauthorized Modification of Information | Probability | 3 | Restricted access; run sheet review; automated file review | Mostly Effective | **Low** |
| | Severity | C | **Medium** | | |
| System Tampering | Probability | 3 | SDLC processes; video camera review | Mostly Effective | **Low** |
| | Severity | C | **Medium** | | |

| THREAT | INITIAL THREAT/RISK SCORING | | | CONTROLS/MITIGATION MEASURES | CONTROLS EFFECTIVENESS | RESIDUAL RISK SCORE |
|---|---|---|---|---|---|---|
| **UNABLE TO TRANSMIT ACH DATA FILES:  NATURAL AND ELEMENTAL THREATS** | | | | | | |
| Flooding | Probability | 2 | **Low** | Sump pump, moisture sensors | Moderately Effective | **Low** |
| | Severity | D | | | | |
| Earthquake | Probability | 2 | **Low** | Large Scale Absence Policy | Mildly Effective | **Very Low** |
| | Severity | C | | | | |
| Electrical Storm (Lightning) | Probability | 4 | **Medium** | Generators; Power Interruption Plan | Mostly Effective | **Low** |
| | Severity | B | | | | |
| Severe Winds/Tornado | Probability | 2 | **Low** | Shelter-in-place procedures | Moderately Effective | **Low** |
| | Severity | D | | | | |
| Snow/Blizzard | Probability | 4 | **Medium** | Remote Work; Delayed Starts | Mostly Effective | **Low** |
| | Severity | B | | | | |
| Severe Winter Storm | Probability | 3 | **Very Low** | Remote Work; Generators | Mostly Effective | **Very Low** |
| | Severity | A | | | | |
| Freezing | Probability | 3 | **Low** | Remove ice buildup on essential equipment | Moderately Effective | **Low** |
| | Severity | B | | | | |
| Severe Heat | Probability | 2 | **Low** | Datacenter HVAC, office building cooling units | Mostly Effective | **Very Low** |
| | Severity | C | | | | |
| Fire | Probability | 2 | **Low** | Hydrants located around building, Fire suppression system, annual evacuation test | Moderately Effective | **Very Low** |

| THREAT | INITIAL THREAT/RISK SCORING | | | CONTROLS/MITIGATION MEASURES | CONTROLS EFFECTIVENESS | RESIDUAL RISK SCORE |
|---|---|---|---|---|---|---|
| **UNABLE TO TRANSMIT ACH DATA FILES:  UTILITY FAILURE** | | | | | | |
| Commercial Power Failure | Probability | 2 | **Low** | Generators, Power Interruption Plan, Remote Work Solution | Mostly Effective | **Very Low** |
| | Severity | E | | | | |
| Loss of NG Supply to Building | Probability | 1 | **Very Low** | Large Scale Absence Policy | Mildly Effective | **Very Low** |
| | Severity | D | | | | |
| Data Communications Disruption | Probability | 2 | **Low** | Redundant ISP and network appliances. | Mostly Effective | **Low** |
| | Severity | D | | | | |
| Voice Communications Disruption | Probability | 2 | **Low** | Redundant ISP and network appliances | Mostly Effective | **Low** |
| | Severity | D | | | | |
| Loss of Water/Sewer Services | Probability | 2 | **Very Low** | Remote work, bottled water, rent porta potties | Mostly Effective | **Very Low** |
| | Severity | B | | | | |

| THREAT | INITIAL THREAT/RISK SCORING | | | CONTROLS/MITIGATION MEASURES | CONTROLS EFFECTIVENESS | RESIDUAL RISK SCORE |
|---|---|---|---|---|---|---|
| **UNABLE TO TRANSMIT ACH DATA FILES: EQUIPMENT FAILURE** | | | | | | |
| Internal Power Failure (loss of UPS) | Probability | 2 | Low | Preventative Maintenance Checks and Services (PMCS) | Mostly Effective | **Very Low** |
| | Severity | E | | | | |
| Heating Ventilation and Cooling Failure | Probability | 2 | Low | Warranty service and support for datacenter HVAC, vendor and landlord support for building HVAC ; temporary HVAC systems | Mostly Effective | **Very Low** |
| | Severity | C | | | | |
| Network Infrastructure | Probability | 2 | Low | Appliance Replacement agreements, warranty service | Mostly Effective | **Very Low** |
| | Severity | D | | | | |
| IT Systems Failure | Probability | 2 | Low | Replacement agreements, warranty service, HA plan for PROD | Mostly Effective | **Very Low** |
| | Severity | D | | | | |

# Life Cycle Stage: Data at Rest

*Governing Policy or Procedures: Information Security Program*

| THREAT | INITIAL THREAT/RISK SCORING | | | CONTROLS/MITIGATION MEASURES | CONTROLS EFFECTIVENESS | RESIDUAL RISK SCORE |
|---|---|---|---|---|---|---|
| **ADDITIONAL CONTROLS: SECURITY THREATS** | | | | | | |
| Physical Theft of Hardware | Probability | 2 | **Medium** | Physical access controls; restricted access to data centers; background checks on employees | Moderately Effective | **Medium** |
| | Severity | E | | | | |
| Improper Handling of Sensitive Information | Probability | 2 | **Medium** | Technical controls on electronic data, including encryption and access by job role | Moderately Effective | **Medium** |
| | Severity | D | | | | |
| Social Engineering | Probability | 5 | **Very High** | Awareness training, firewall controls, web filters | Mostly Effective | **Medium** |
| | Severity | E | | | | |
| Unauthorized External Access | Probability | 2 | **Medium** | Firewall, whitelisting, vulnerability management and intrusion detection | Mostly Effective | **Medium** |
| | Severity | E | | | | |
| Unauthorized Internal Access | Probability | 2 | **Medium** | Least privilege access; limited FedLine access; application login and menu controls; background checks on employees; library segregation | Mostly Effective | **Medium** |
| | Severity | D | | | | |
| Falsified Input | Probability | 2 | Very Low | Application login controls, including limitations of access and individualized logins | Moderately Effective | **Very Low** |
| | Severity | B | | | | |
| Negligence or Human Error | Probability | 1 | Very Low | Run sheet review; automated ROBOT processing; control testing | Mostly Effective | **Low** |
| | Severity | D | | | | |
| Unauthorized Modification of Information | Probability | 3 | **Medium** | Restricted access; run sheet review; automated file review | Mostly Effective | **Low** |
| | Severity | C | | | | |
| System Tampering | Probability | 3 | **Medium** | SDLC processes; video camera review | Mostly Effective | **Low** |

See above for controls related to natural and elemental, utility failure, and equipment failure threats.

# Life Cycle Stage: Data on Backups

*Governing Policy or Procedures: Information Security Program*

| THREAT | INITIAL THREAT/RISK SCORING | | | CONTROLS/MITIGATION MEASURES | CONTROLS EFFECTIVENESS | RESIDUAL RISK SCORE |
|---|---|---|---|---|---|---|
| **ADDITIONAL CONTROLS: SECURITY THREATS** | | | | | | |
| Physical Theft of Hardware | Probability | 2 | **Medium** | Physical access controls; restricted access to data centers; background checks on employees | Moderately Effective | **Medium** |
| | Severity | E | | | | |
| Improper Handling of Sensitive Information | Probability | 2 | **Medium** | Technical controls on electronic data, including encryption and access by job role; third-party vendor for document destruction is part of vendor review | Moderately Effective | **Medium** |
| | Severity | D | | | | |
| Social Engineering | Probability | 5 | **Very High** | Awareness training, firewall controls, web filters | Mostly Effective | **Medium** |
| | Severity | E | | | | |
| Unauthorized External Access | Probability | 2 | **Medium** | Firewall, whitelisting, vulnerability management and intrusion detection | Mostly Effective | **Medium** |
| | Severity | E | | | | |
| Unauthorized Internal Access | Probability | 2 | **Medium** | Least privilege access; limited FedLine access; application login and menu controls; background checks on employees; library segregation | Mostly Effective | **Medium** |
| | Severity | D | | | | |
| Falsified Input | Probability | 2 | **Very Low** | Application login controls, including limitations of access and individualized logins; system checks to ensure correct data is transmitted to backup data and media is functional; | Moderately Effective | **Very Low** |
| | Severity | B | | | | |
| Negligence or Human Error | Probability | 1 | **Very Low** | Run sheet review; automated ROBOT processing; control testing; CU*Answers can reproduce ACH transactions in the event if necessary; CU*Answers has a Records and Information Program to prevent destruction of data prior to retention expiration | Mostly Effective | **Low** |
| | Severity | D | | | | |
| Unauthorized Modification of Information | Probability | 3 | **Medium** | Restricted access; run sheet review; automated file review | Mostly Effective | **Low** |
| | Severity | C | | | | |
| System Tampering | Probability | 3 | **Medium** | SDLC processes; video camera review | Mostly Effective | **Low** |

See above for controls related to natural and elemental, utility failure, and equipment failure threats.

# Life Cycle Stage: Data in Transit to Client

CU*Answers does not have risks independent from the Federal Reserve.

| THREAT | INITIAL THREAT/RISK SCORING | | | CONTROLS/MITIGATION MEASURES | CONTROLS EFFECTIVENESS | RESIDUAL RISK SCORE |
|---|---|---|---|---|---|---|
| **FEDERAL RESERVE** | | | | | | |
| N/A | Probability | N/A | **N/A** | N/A | N/A | **N/A** |
| | Severity | N/A | | | | |

# Risk Assessment Key

This Risk Assessment regards probability in five grades: Very Low, Low, Medium, High, and Very High. Severity is graded using the same ranking system. Point values are assigned to each level of probability and severity. A heat map value has also been created to reflect the weight of the respective threat's total Probability and Severity.

Threat Impact Probability is rated using this list of perceived probabilities:

| Threat Impact Probability | Chance of Occurrence |
|---|---|
| Very Low | 1-10% |
| Low | 11-30% |
| Medium | 31-60% |
| High | 61-85% |
| Very High | 86-100% |

The Impact Severity is rated using this key:

| Threat Impact Severity | Impact |
|---|---|
| Very Low | Recovery Time Objectives (RTOs) not likely to be affected |
| Low | May affect three or more business functions and stress their RTOs |
| Medium | Threat may affect many business functions |
| High | Threats of this level will affect most business functions and their RTOs |
| Very High | Will affect RTOs of the entire organization |

*Recovery Time Objective is the maximum acceptable time it takes to restore a system or application after an outage.*

Controls are measured as follows:

| Types of Controls | Controls Effectiveness |
|---|---|
| Administrative | Fully |
| Technical | Mostly |
| Physical | Moderately |
| Detective | Partially |
| Preventative | Mildly |

This matrix determines the severity of risk:

| Probability | Severity | | | | |
|---|---|---|---|---|---|
| | Insignificant (A) | Minor (B) | Moderate (C) | Major (D) | Catastrophic (E) |
| Almost Certain (5) | 5A | 5B | 5C | 5D | 5E |
| Occasional/Likely (4) | 4A | 4B | 4C | 4D | 4E |
| Uncommon (3) | 3A | 3B | 3C | 3D | 3E |
| Rare (2) | 2A | 2B | 2C | 2D | 2E |
| Improbable (1) | 1A | 1B | 1C | 1D | 1E |

This heat map matrix is used after determining the probability and severity level of each threat within the previous matrix:

| Probability | Severity | | | | |
|---|---|---|---|---|---|
| | Very Low (1) | Low (2) | Medium (3) | High (4) | Very High (5) |
| Very High (5) | Medium | High | Very High | Very High | Very High |
| High (4) | Low | Medium | High | High | High |
| Medium (3) | Very Low | Low | Medium | Medium | Medium |
| Low (2) | Very Low | Very Low | Low | Low | Low |
| Very Low (1) | Very Low | Very Low | Very Low | Very Low | Very Low |

# Risk Assessment Definitions

## SECURITY THREATS

| THREAT | DESCRIPTION |
|---|---|
| Physical Theft of Hardware | Acquisition of data, hardware and/or software by unauthorized individuals. |
| Improper Handling of Sensitive Information | The failure of authorized individuals to handle sensitive information (e.g., Privacy Act protected, Sensitive but Unclassified, For Official Use Only, proprietary, etc.) in accordance with applicable policies and procedures, possibly compromising the information. |
| Social Engineering | A method of obtaining information to be used for compromising a system (e.g., a password) from an individual rather than by breaking into the system. Social engineering can be used over an extended period to maintain a continuing stream of information and help unsuspecting users. |
| Unauthorized External Access | The ability and opportunity of an external source to obtain information or physical access to facilities without proper authorization or clearance. |
| Unauthorized Internal Access | The ability and opportunity of an internal source to obtain information or physical access to facilities without proper authorization or clearance. |
| Falsified Input | Deliberately inputting inaccurate data or information into a system to cause corruption of data. |
| Negligence or Human Error | Failure to act carefully and responsibly, resulting in unintended destruction or degradation to the system. |
| Unauthorized Modification of Information | A technique used to reduce network overhead by having devices, such as bridges and routers, answer for remote devices or by manipulating internet protocol (IP) addresses, so that the attacker appears to be someone or something else. |
| System Tampering | Interfering with the system in a harmful manner resulting in degradation or unavailability of system and/or resources. |

## NATURAL AND ELEMENTAL

| THREAT | DESCRIPTION |
|---|---|
| **Flooding** | Flooding of the computer room and support areas from sources external to the building (e.g., retention ponds, etc.). |
| **Earthquake** | An earthquake causing structural damage to the facility and surrounding area. |
| **Electrical Storm (Lightning)** | A lightning strike can cause a power surge and damage electrical delivery equipment. |
| **Severe Winds/Tornado** | Facility and/or surrounding area damage due to high winds, tornadoes, and hail not directly associated with other natural threats. |
| **Snow/Blizzard** | Conditions which lead to heavy snowfall, and blizzard conditions. |
| **Severe Winter Storm** | Conditions which lead to heavy snowfall, and ice conditions which may threaten commute and working conditions. |
| **Freezing** | Freezing conditions, including Ice precipitation. |
| **Severe Heat** | Severe Heat waves can affect the operation of equipment and availability of personnel. |
| **Fire** | Can include large fires (e.g., those that trigger the fire suppression system, if the site is so equipped, or require the involvement of trained firefighters) and small fires (e.g., those extinguishable with a hand-held extinguisher). |

## UTILITY FAILURE

| THREAT | DESCRIPTION |
|---|---|
| **Commercial Power Failure** | Long-term power failure associated with power outages. |
| **Loss of NG Supply to Building** | Disruption to Natural Gas supply. |
| **Data Communications Disruption** | Loss or disruption of data communication capabilities. |
| **Voice Communications Disruption** | Loss or disruption of telephonic communication capabilities. |
| **Loss of Water/Sewer Services** | Disruption to the function of Water Supply, and/or Sewer availability. |

## EQUIPMENT FAILURE

| THREAT | DESCRIPTION |
|---|---|
| **Internal Power Failure (loss of UPS)** | Loss of Uninterruptible Power Supply. |
| **Heating Ventilation and Cooling Failure** | Failure of environmental controls, causing increased temperature and humidity, which can damage sensitive computer equipment and storage media. |
| **Network Infrastructure** | Threat stemming from failure of network systems and equipment necessary to provide data and voice communications to staff. |
| **IT Systems Failure** | Failure or inadequacy of operational information systems. |

**The Clearing House®**

July 11, 2025

Geoff Johnson
CU*Answers
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' ACH activity was performed on May 27 - 30, 2025, to verify compliance with the ACH Operating Rules.  The audit sample period covered March 3 - 14, 2025.

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, 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. 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

The Clearing House Payments Authority   580 Kirts Boulevard, Suite 301, Troy, MI 48084   Phone 800.875.2242, option 3   Fax 336.769.5355   www.theclearinghouse.org

TCH CONFIDENTIAL

## 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 May 27th – 30th, 2025. The audit sample period included March 3rd-14th. 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.

Sarah Reamer, APP
Payments Compliance
The Clearing House Payments Authority

Reviewed By:  Joe Allen, AAP
                        June 12, 2025

# 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 audits were provided for review for 2019-2024. 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 protect DFI account numbers used in the initiation of Entries by rendering them unreadable when stored electronically by June 30 of the year immediately following the year in which such volume first exceeds the 2 million entry threshold, and consistently thereafter regardless of the annual volume.*

**Status:**     *Compliant*

**Comments:**  CU*Answers maintains Cyber Security, Information Security, and Physical Security policies.  Data security, storage and destruction of data is identified within the policies.  CU*Answers partners with a third-party vendor to conduct annual SOC reports; data security is included within the report.

### *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 are 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.*

*The Third-Party Sender may choose, at its discretion, to make the changes specified in any NOC or corrected NOC received with respect to any Single Entry.*

**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 it's NOCs and exceptions. The Credit Unions transmit outgoing NOCs 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.

# The Clearing House®

## 2025 ACH Audit Certification

Company Name:  CU*Answers

Date of Audit:   May 24th- 30th, 2025

Audit Sample Period:  March 3rd-14th, 2025

Auditor Name:  Sarah Reamer, 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

The Clearing House 1114 Avenue of the Americas, 17th Floor, New York, NY 10036 Phone 212.613.0100 Fax 212.613.9811 www.theclearinghouse.org

TCH CONFIDENTIAL