AuditLink

2022 Annual ACH Risk Assessment

CU*Answers

September 29, 2022

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

Patrick Sickels, CISA, CRISC
Internal Auditor
6000 28th St SE
Grand Rapids, MI
800-327-3478 ext.335
psickels@cuanswers.com

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, 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.

September 29, 2022
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 September 20, 2022, fourteen employees are authorized FedLine token holders (CU*Answers' Operations Team and Xtend, Inc.).

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 Eastern Time.

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 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 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 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

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 CU*Answers' 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

AuditLink

2022 Annual ACH Audit

CU*Answers

September 29, 2022

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

CU*ANSWERS Management Services

PURPOSE

An objective, comprehensive evaluation of CU*Answers ACH policies, procedures and processes was conducted on September 24th, 2022.

The overall objective was to assess ACH Compliance with respect to the 2022 NACHA Operating Rules relative to those that apply to Third Party Service Providers. CU*Answers is a CUSO serving the national credit union marketplace. CU*Answers flagship product is a core banking application which processes incoming ACH items from the Federal Reserve and sends back those items credit unions have set to a return status.

The annual ACH audit of the CUSO consists of audit findings, observations, recommendations, and violations, if applicable. The areas under review include annual audits and retention thereof, security of electronic networks used to process activity, risk assessment and security of protected information, provisions for internal third party sending of ACH transactions, obligations for providing required information for specific entries, and timing requirements to post entries.

Based upon the sampling review of the above items CU*Answers was found to be **in compliance in all areas with no exceptions noted.**

Audits

Verify that CU*Answers has conducted an audit of compliance with the ACH Rules and retained for a period of six years. Ensure that any Third-Party Service Providers affiliated with CU*Answers has also had an ACH audit performed annually.

Findings/Recommendations: CU*Answers has had an ACH audit performed by December 31 of every year for the last six years as evidenced by the review of the audits provided by the CU*Answers internal audit team.

Third party ACH audits obtained and reviewed included:

Magic-Wrighter – 2021 – No findings.

Payveris – 2022, Certificate of Completion performed by NEACH.

Alloya – 2021 – No findings. Currently going through 2022 Audit and expected to be completed by the end of September 2022.

Site-Four – 2021 – No findings.

Jack Henry - iPay – No findings.

Some of the above vendors are also part of the vendor management program CU*Answers has instituted for ongoing monitoring of these vendors which is completed by Patrick Sickels utilizing the AuditLink division.

There were no findings and recommendations from the prior year's CU*Answers audit which required remediation.

Record Retention

Verify that all ACH records, including received, returned and originated entries are securely retained for six years from the date of the entry and access is restricted.

Findings/Recommendations: CU*Answers operations staff provided a sample of various PACXTB ACH reports to prove retention. No exceptions to note.

Secure Transmission of ACH information and Security of Access to the Federal Reserve Network

Verify that required encryption or a secure session is used for banking information transmitted via an Unsecured Electronic Network and for those that have access to the FedLine system. Also verify that access to the FedLine system is managed and maintained related to staff duties and roles.

Findings/Recommendations: CU*Answers provided proof of commercially reasonable encryption levels for the core platform, utilizing a program called Go Anywhere (A2A) and transmissions between CU*Answers, Alloya, Payveris, Magic Writer, Ipay, and FEDLINE. CU*Answers also provided the section of the internal policy manual evidencing the required encryption levels which meet NACHA guidelines. All encryption certificates were reviewed as evidence of the appropriate levels of encryption and no exceptions were noted.

CU*Answers accounting personnel have access to Alloya for the secured transmission from the accounts payable system. An Alloya access report was provided evidencing who is authorized to perform transmissions. All employees that have access are current employees and no exceptions were noted.

CU*Answers has 14 employees with FedLine tokens as evidenced by the Subscriber and Roles Report dated September 20, 2022. 12 token holders are CU*Answers employees and 2 are Xtend SRS bookkeeping employees. Rights for the Xtend employees are limited to performing returns and NOC's. All token holders are current employees, and no users were identified who no longer work for the companies.

CU*Answers also performs two to three high availability roll overs annually to Site-4, located in Yankton, SD. During the rollover ACH files are processed directly from Site-4 using existing tokens of the Grand Rapids staff. The last roll over was performed in July of 2022 and nothing was noted in the gap analysis relating to ACH issues.

Risk Assessment and Security of Protected Information

Verify the participating DFI has conducted an assessment of the risks of its ACH activities and has implemented a risk management program on the basis of such an assessment and has established, implemented, and updated policies and procedures. Verify the Participating Third-Party Service Provider has implemented policies, procedures and systems to protect the confidentiality and integrity of Protected Information.

Findings/Recommendations: CU*Answers conducted a data security assessment on September 1st of 2022. Annual updates are performed as evidenced by prior ACH audits. The 2021 SOC reports are available upon request from Internal Audit. Policies and procedures were obtained and reviewed. CU*Answers ensures ACH data is protected throughout the entire lifecycle.

SOC reports were obtained and have been reviewed for Paymentus (formerly, Payveris), Magic-Wrighter, Jack Henry (iPay), Site-Four, and Alloya. No material exceptions were noted on the reports. CU*Answers SOC was also reviewed with no exceptions noted.

Effective June 30, 2021, NACHA rules dictated that CU*Answers renders account numbers unreadable when the data is at rest. At that time CU*Answers changed the data storage procedures, deleted all prior days saved data, and overwrites the existing file when a new file is received. This was evidenced by a screen print of the storage directory on the IBM iSeries.

ACH Entries Accepted

Verify that all types of entries that comply with these rules and are received with respect to an account maintained with the RDFI are accepted.

Findings/Recommendations: CU*Answers accepts all ACH entries as proven from the PAXTB posting reports listing various SEC codes.

Rights and Responsibilities of ODFIs, Originators and Third-Party Senders

Provisions for Internal Origination

Verify that transactions originated internally are following the related ACH rules.

Findings/Recommendations: Not applicable. CU*Answers does not provide origination services.

CU*Answers is a Third-Party Sender that uses Alloya to originate monthly billing for clients, staff expense reports, and payments to some vendors (accounts payable). The origination contracts are between CU*Answers and the credit union clients. Six employees have access to the Alloya platform and security measures are in place to ensure dual control when setting up a monthly invoice for a client. Entries were reviewed based upon the type of transaction and no exceptions were noted.

Rights and Responsibilities of RDFIs and Their Receivers

Obligation to Provide Information about Entries and Notices to the Receiver for Credit Entries Subject to Article 4A

Verify that required information is made available for each credit and debit Entry to an Account, that the Receiver has been provided proper notice to ensure compliance with UCC 4A and that, when requested, payment related information is provided in a timely manner.

Findings/Recommendations: Samples of client member statements and daily posting reports were provided for review and inspected by AuditLink. We noted that CU*Answers makes the appropriate payment information available to members via the account statement and in the account history on Home Banking. In the event a member requests additional payment information, credit unions can provide that to them directly upon request.

Timing Requirements Make Credit and Debit Entries Available

Verify that all valid ACH transactions are accepted, and consumer credits are made available no later than open of business on Settlement date.

Findings/Recommendations: CU*Answers allows clients to choose to configure up to four posting times and whether they want debits, credits, or both to post. CU*Answers' posting schedule allows for timely posting and ensures Same Day credits are available by 5:00 p.m. In order to verify the posting schedule is adhered to, AuditLink performed a review of the daily run sheets for a sample of days, which evidenced that all postings are completed prior to the required cut off times.