AuditLink

2020
Annual ACH Audit
Risk Assessment
CU*Answers

October 1, 2020

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

Contents

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.

October 1, 2020
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:

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

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

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

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

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

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

Patrick G. Sickels | CU*Answers | Internal Auditor

Update to 2019 ACH Audit Findings

CU*Answers remediated the 2019 finding at the time the finding was disclosed. AuditLink confirmed during the 2020 audit that this finding was fully remediated.

Originator Obligations

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

Status of audit requirement: Compliant with Exception

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

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

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

2020 ACH Audit Findings

No findings.

ACH Data Flows

DAILY ACH FILES RECEIVED VIA CU*BASE

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

ORIGINATED A2A AND MOP VIA MAGICWRIGHTER

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

ACCOUNTING INVOICE ORIGINATION

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

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

ACH Risk Assessments

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

Governing Policy or Procedures: Operations Run Sheets

INHERENT RISKS	RISK RATING	CONTROLS	RESIDUAL RISKS	RESIDUAL RATING
Data could be exposed to parties not authorized to see it	**HIGH**	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**

Audit Purpose

An objective, comprehensive evaluation of CU*Answers ACH policies, procedures and processes was conducted on July 31, 2020.

The overall objective was to assess ACH Compliance with respect to the 2018 NACHA Operating Rules; Appendix Eight Part 8.1 - General Audit Requirements for Participating Depository Financial Institutions, Part 8.2 - Audit Requirements of Participating Financial Institutions, Part 8.3 – Audit Requirements for RDFI's

The annual ACH audit of the credit union consists of audit findings, observations, recommendations, and violations, if applicable, with a conclusion.

General Audit Requirements – Article One

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 no later than December 31 of every year for the last six years as evidenced by the review of the audits contained in the internal audit directory. No Exceptions to note.

Third party audits obtained and reviewed included:

Magic-Wrighter: 2019–2020

Payeris: 2019

Alloya: 2019-2020

Vizo (MY CU Services): December 2019

Site-Four: 2019

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

Findings and recommendations from the prior audits were addressed and remedied. Proof of the finding regarding accounts payable ACH origination regarding standard entry class codes was obtained by reviewing raw transmission data against the posting report and member account.

Record Retention

Verify that all ACH records, received, returns 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 via Unsecured Electronic Networks and Security of Access to the FedLine system

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

Findings/Recommendations: CU*Answers provided proof of commercially reasonable encryption levels for the core platform, avenues utilizing a program called Go Anywhere (A2A and transmissions between CU*A and My CU Services, Alloya, Payveris, Magic Writer, Ipay, Fed Line, and Gold. No Exceptions to note.

CU*Answers accounting personnel have access to Alloya for the secured transmission for the accounts payable system. A Alloya report was provided showing who is authorized and termination checklist for people with access rights.

CU*Answers has 10 employees with FedLine tokens as evidenced by the Subscriber and Roles Report dated 7/27/2020. All token holders are current employees and no users were identified who no longer work for the company.

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 in October of 2019 and annual updates are performed with the last being August 1st of 2020. The 2018 SOC reports are available on the company website. Policies and Procedures were obtained and reviewed. CU*Answers does ensure that ACH data is protected throughout the entire lifecycle. No Exceptions to note.

SOC reports were obtained and have been reviewed from Payveris, Magic-Wrighter, and Vizo. Alloya provided their annual audit and do not perform a SOC. These can be found and were verified in CU*Answers vendor management portal.

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. No Exceptions to note.

Rights and Responsibilities of ODFIs, Originators and Third-Party Senders – Article Two

Provisions for Internal Origination

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

Findings/Recommendations: CU*Answers does not provide origination services to their clients.

CU*Answers is a Third-Party Sender as they use Alloya to originate their monthly billing for their clients and staff expense reports. The origination contracts are between CU*Answers and the credit union clients. CU*A also holds an origination contract with Alloya. Four 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. Two employees are required to send an invoice. No Exceptions to note.

Rights and Responsibilities of RDFIs and Their Receivers – Article Three

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 were provided for review. CU*Answers does make the appropriate payment information available to members via the account statement and in the account history on Home Banking. No Exceptions to note.

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 three posting times and whether they want debits, credits or both to post. CU*A posting schedule allows for timely posting and ensures Same Day credits are available by 5:00pm. A random review of the morning posting file proved all morning postings are completed by the beginning of the business day. No Exceptions to note.