AuditLink

CU*ANSWERS
A Credit Union Service Organization

CU*ANSWERS
FY2018
ACH RISK ASSESSMENT

October 16, 2018

OVERVIEW

The National Automated Clearing House Association ("NACHA") Rule on Section 1, 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

Marsha Sapino AAP, BSACS | CU*Answers | AuditLink Assistant Manager

ACH LIFE CYCLE DATA FLOW

Daily ACH Files Received

- CU*Answers receives multiple ACH files throughout the day via FedLine
- Currently, twelve employees are authorized FedLine token holders (Operations)
- 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 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 Planes 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

RISK ASSESSMENT

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**	*System will not function without encryption*	*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 of time*	**LOW**	*Tested annually through the DR/BR with complete 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**	*Vender 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**

2018 Annual ACH Audit

CU*Answers

October 16, 2018

Marsha Sapino, AAP, BSACS
AuditLink Assistant Manager
6000 28th St SE
Grand Rapids, MI
800-327-3478 ext.380
Marsha.sapino@cuanswers.com

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

PURPOSE

An objective, comprehensive evaluation of CU*Answers ACH policies, procedures and processes was conducted on September 2018.

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 bi-annual internal ACH audit of CU*Answers consists of audit findings, observations, recommendations, and violations, if applicable, with a conclusion.

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.

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 annual ACH audit every year for the last six years. Proof of retention was obtained. Magic-Wrighter, Payeris, Alloya and Mid-Atlantic provided proof of their annual audits.

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 provided a sample of various ACH reports to prove out retention. No Exceptions to note.

Secure Transmission of ACH information via Unsecured Electronic Networks

Verify that required encryption or a secure session is used for banking information transmitted via an Unsecured Electronic Network

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*Answers and Mid Atlantic), FedLine and Alloya. CU*Answers uses an application called Great Plains to upload ACH data to Alloya for invoice origination. That activity is performed behind the CU*Answers secure firewall.

CU*Answers has 12 employees with FedLine tokens. All token holders are still current employees. However, one employee's token had expired in May 2018 but was still showing as active. CU*Answers is in the process of deactivating that token.

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 February 2018 and their 2017 SSAE reports are available on the company website. Policies and Procedures were obtained and reviewed. These Policies do ensure that ACH data is protected. SOC reports were obtained from Payveris, and Magic-Wrighter provided proof that their SOC is current. Alloya provided their annual audit.

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.

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

Provisions for Internal Origination

Verify that transactions originated internally are in compliance with the related ACH rules.

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

CU*Answers is a Third-Party Sender because they use Alloya to originate their monthly billing for their clients. The origination contracts are between CU*Answers and the credit union clients. CU*Answers 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.

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 makes the appropriate payment information available to members via the account statement and in the account history on Home Banking.

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*Answers posting schedule allows for timely posting and ensures Same Day credits are available by 5:00pm.