CU*ANSWERS
A CREDIT UNION SERVICE ORGANIZATION

MEMORANDUM

December 7, 2015

To: CU*Answers Executive Council
CU*Answers Board of Directors

From: Patrick Sickels
Internal Auditor
CU*Answers

Re: ACH Audit 2015

Attached is the 2015 ACH audit. Every other year we have an external audit firm perform the ACH audit, and in 2015 this audit was performed by The Payments Authority. We engage with The Payments Authority as we believe they are the premier trade association for understanding ACH requirements. External audits are not required by law, but it is the opinion of CU*Answers and our Board of Directors that a bi-annual external audit best serves our organization and our clients.

Marsha Sapino, AAP, is the primary CU*Answers' employee working with The Payments Authority. Marsha works closely with Jim Vilker, NCCO, who heads up CU*Answers' Audit Link division. The responsibility of the audit ultimately falls under the purview of the CU*Answers Internal Audit department.

There are three items in the 2015 ACH Audit. The first is not a finding, as confirmed by The Payments Authority. The second finding is retention of the assent and authorization language; we implemented this change in 2015 and are compliant going forward. Finally, there is a relatively new requirement for a self-assessment on processing and destruction of ACH records. We had not completed this at the time of the audit. This is now complete, verified, and attached to this report. Please note, if you as a financial institution have not completed your own ACH risk assessment, AuditLink can assist with this requirement.

We are pleased with the audit and the work our teams do to keep us compliant and secure.

ATTESTATION

Neither management nor the board of directors improperly influenced the findings in this report.

Patrick G. Sickels

Patrick G. Sickels, Internal Auditor, CU*Answers

FINDINGS SUMMARY

8.1 General Audit Requirements

Recommendations/Concerns

*Magic Wrighter is a Sending Point for CU*Answers for Account to Account transfers. The member credit union that offers the service is the ODFI. Credit Union's do not have a contract with CU*Answers for A to A transactions transmitted by Magic Wrighter.*

The Bill Pay services offered via Fiserv are outsourced and the credit union is not the ODFI of these transactions.

Management Response: This is a not a finding, confirmed with The Payments Authority.

8.2B Electronic Records

Finding: **Compliant with Exceptions**

Account to Account transactions are offered to member credit unions via the home banking platform. Members may make debit or credit transfers known as "Right Now Payments". Recurring transactions are not currently permitted. The date, time, length of session, and IP address is captured and retained. Authorization language has been added to A to A in 2015.

Exception: The assent and authorization language cannot be reproduced in 2013 and 2014 as required by the E-Sign Act and the ACH rules.

Management Response: Our software was modified in 2015 to allow for the assent and authorization language.

8.2G Security of Protected Information

Finding: **Non-Compliant**

*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. Note:(3) does not apply to CU*Answers*

Although policies have been updated to include the ACH Data Security; a self-assessment has not been conducted of the initiation, processing, storage and destruction of ACH entries and records. Note: The destruction of ACH data from the Operations Department is outsourced. This process should be considered during the self-assessment.

Note: The ACH data held by the CUSOs should be included in the self-assessment.

Management Response: We had not completed a compliant assessment as was new in 2014. We have attached the assessment and confirmed our compliance with The Payments Authority.

AuditLink

CU*ANSWERS
A Credit Union Service Organization

CU*ANSWERS
2015 ACH RISK ASSESSMENT

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 the 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, and include those 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.

Ultimately, risks and results of our ACH audits are made public to our clients, their auditors and examiners, so that they 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 Associate

RISK ASSESSMENT

LIFE CYCLE STAGE: DATA IN TRANSIT TO AND FROM THE FEDERAL RESERVE

GOVERNING POLICY OR PROCEDURES: OPERATIONS RUN SHEETS

INHERENT RISKS	RESIDUAL RISKS
Data could be exposed to parties not authorized to see it	The likelihood that our 128bit encryption level could be cracked
Communication lines between the Fed and CUA are damaged for an extended period of time	Would not be able to receive the files in a timely manner.
CONTROLS	CONTROLS
Monitoring the integrity of encryption protocols.	Tested annually through the DR/BR with complete gap analysis reported to the Board of Directors
OVERALL RISK	OVERALL RISK
LOW	MODERATE

LIFE CYCLE STAGE: DATA IN TRANSIT TO CLIENT (WOULD INCLUDE DELIVERY TO CLIENT AND MOVEMENT BETWEEN SERVERS INTERNALLY)

GOVERNING POLICY OR PROCEDURES: OPERATIONS RUN SHEETS

INHERENT RISKS	RESIDUAL RISKS
Same as the Federal Reserve	Same as the Federal Reserve
OVERALL RISK	OVERALL RISK
SAME AS THE FEDERAL RESERVE	SAME AS THE FEDERAL RESERVE

LIFE CYCLE STAGE: DATA AT REST ON I-SERIES AND EDOC SERVERS

GOVERNING POLICY OR PROCEDURES: INFORMATION SECURITY PROGRAM

INHERENT RISKS	RESIDUAL RISKS
Same as the Federal Reserve	Malicious hacks into our network
Same as the Federal Reserve	Internal Employee risk
Same as the Federal Reserve	ACH Data left out into the open
CONTROLS	CONTROLS
Same as the Federal Reserve	Firewall maintenance and patch management stays updated and current.

	Annual penetration tests with complete gap analysis.
	Complete background checks for new hires along with strong system security policies. Strict policies with audit functionality relating to sensitive data left in the public eye.
OVERALL RISK	OVERALL RISK
SAME AS THE FEDERAL RESERVE	MODERATE

LIFE CYCLE STAGE: DATA AT REST AND BACKUP

GOVERNING POLICY OR PROCEDURES: INFORMATION SECURITY PROGRAM

INHERENT RISKS	RESIDUAL RISKS
Same as the Federal Reserve	Theft of the media along with cracking of the encryption or the password keys get stolen
Destruction of the data prior to our retention requirement	Risk of someone breaking into the facilities or unintended loss while data being transported to the facility
Backup media failure	Unable to reproduce ACH transactions in the event it would be necessary to repost a file or perform an investigation
CONTROLS	CONTROLS
Same as the Federal Reserve	Encryption key is not on site
All backups are encrypted	Multiple physical controls prevent access to our backup media
System has checks to ensure backup media is functional	There is multiple backup systems in the event of a single system failure
OVERALL RISK	OVERALL RISK
LOW	LOW

LIFE CYCLE STAGE: DATA IN STORAGE REPORTS

GOVERNING POLICY OR PROCEDURES: INFORMATION SECURITY PROGRAM

INHERENT RISKS	RESIDUAL RISKS
Same as the Federal Reserve	Unauthorized access to ACH information
CONTROLS	CONTROLS
Same as the Federal Reserve	Library software allows financial institutions to control who can see and access reports
OVERALL RISK	OVERALL RISK
SAME AS THE FEDERAL RESERVE	LOW

LIFE CYCLE STAGE: DATA DESTRUCTION

GOVERNING POLICY OR PROCEDURES: RIM POLICY

INHERENT RISKS	RESIDUAL RISKS
Exposure to unauthorized individuals	Destruction company steals the data
CONTROLS	CONTROLS
Library software allows financial institutions to control who can see and access reports	Vender management program including legal review of contract, physical site audit, review of insurance and bonding of company
OVERALL RISK	OVERALL RISK
LOW	LOW

THE Payments AUTHORITY

October 16, 2015

Patrick Sickels
CU*Answers
6000 28th St., Ste. 1000
Grand Rapids, MI 49546

Dear Patrick,

Thank you for the hospitality shown to me during my visit at CU*Answers. It was a pleasure visiting with your staff. Each participating DFI and Third Party Provider shall, in accordance with standard auditing procedures, conduct annually an internal or external audit of compliance with the provisions of the ACH rules in accordance with the requirements of Appendix Eight of the 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.

The external audit of CU*Answers ACH Operations was performed on September 2 - 3, 2015 to verify compliance with the *ACH Operating Rules* and to meet audit requirements as detailed in Appendix Eight of the *ACH Operating Rules*. The audit period covered July 22 through August 5 and September 1 through 2, 2015. Any suggestions or follow-up items 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. This audit was based on selective sampling of various disclosures, and documents pertaining to ACH and a review of compliance with NACHA rules and guidelines. Conclusions were based on the results of the information reviewed, discussion with various employees and personal observations.

The ACH Audit Management Report is intended solely for the information and use of CU*Answers, The Payments Authority and the National Automated Clearing House Association. Below is a summary of audit findings and recommendations. For detailed information, please review the attached complete ACH Audit Management Report. This report is to be used as evidence of performance of the ACH Audit for the calendar year ending December 31, 2015.

ACH Audit: The audit was conducted on a selective sampling, and it is noted that there was one Noncompliance finding. There are audit requirements that are noted as Compliance with Exception or Compliance with Follow-up. These areas are addressed in the ACH Audit Management Report.

Thank you for contracting with The Payments Authority to conduct your annual audit.

Sincerely,

Meg Prieur

Meg Prieur, AAP
Education and Professional Services

ACH Audit Management Report

Institution Name: CU*Answers

RTN: 6724 6024 3

Date of Audit: September 2-3, 2015 RDFI □ ODFI □

Audit Period: July 22-August 5, and September 1-2, 2015

Auditor Name: Meg Prieur, AAP

Third-Party Provider	Verification of Audit
Magic Wrighter (AtoA)	☑
Fiserv (Ipay)	☑
	□
	□
	□
	□

8.1 General Audit Requirements

Each Participating DFI, Third-Party Service Provider, and Third-Party Sender must, in accordance with standard auditing procedures, conduct an internal or external audit of compliance with provisions of the ACH rules in accordance with the requirements of this Appendix Eight. These audit provisions do not prescribe a specific methodology to be used for the completion of an audit but identify key rule provisions that should be examined during the audit process.

An annual audit must be conducted under these Rule Compliance Audit Requirements no later than December 31 of each year. This audit must be performed under the direction of the audit committee, audit manager, senior level officer, or independent (external) examiner or auditor of the Participating DFI, Third-Party Service Provider, or Third- Party Sender. The Participating DFI, Third-Party Service Provider or Third Party Sender must retain proof that is has completed an audit of compliance in accordance with these rules. Documentation support the completion of an audit must be (1) retained for a period of six years from the date of the audit, and (2) provided to the National Association upon request. Failure of a Participating DFI to provide proof of completion of an audit according to procedures determined by the National Association may be considered a Class 2 rule violation pursuant to Appendix Ten, subpart 10.4.7.4 (Class 2 Rules Violation).

Recommendations/Concerns

Magic Wrighter is a Sending Point for CU*Answers for Account to Account transfers. The member credit union that offers the service is the ODFI. Credit Union's do not have a contract with CU*Answers for A to A transactions transmitted by Magic Wrighter.

The Bill Pay services offered via Fiserv are outsourced and the credit union is not the ODFI of these transactions.

8.2 Audit Requirements for All Participating DFIs

Each Participating DFI, Third-Party Service Provider, and Third-Party Sender must conduct the following audit of ACH operations. These audit specifications apply generally to all Participating DFIs, regardless of a Participating DFI's status as an ODFI or RDFI.

8.2A Record Retention

Verify that a Record of each Entry is retained for six years from the date the Entry was Transmitted, except as other- wise expressly provided in these Rules. Verify that a printout or reproduction of the information relating to the Entry can be provided, if requested by the Participating DFI's customer or any other Participating DFI or ACH Operator that originated, Transmitted, or received the Entry. (Article One, subsections 1.4.1 and 1.4.2)

Finding: **Does Not Apply**

Recommendations/Concerns

CU*Answers is not required to retain ACH records.

8.2B Electronic Records

When a Record required by these Rules is created or retained in an Electronic form, verify that the Electronic form (a) accurately reflects the information in the Record, and (b) is capable of being accurately reproduced for later refer ence, whether by Transmission, printing, or otherwise.(Article One, subsection 1.4.3)

Finding: **Compliant with Exceptions**

Recommendations/Concerns

Account to Account transactions are offered to member credit unions via the home banking platform. Members may make debit or credit transfers known as "Right Now Payments". Recurring transactions are not currently permitted. The date, time, length of session, and IP address is captured and retained. Authorization language has been added to A to A in 2015.

Exception: The assent and authorization language can not be reproduced is 2013 and 2014 as required by the E-Sign Act and the ACH rules.

8.2C Previous Year Audits

Verify that the Participating DFI conducted an audit of its compliance with the Rules in accordance with Appendix Eight (Rule Compliance Audit Requirements) for the previous year. (Article One, subsection 1.2.2)

Finding: **Compliant**

Recommendations/Concerns

Verified an ACH audit was conducted October 2014.
Note: To comply with ACH record retention of audits, procedures should address retention of ACH audits for 6 years.

8.2D Encryption

Verify that required encryption or a secure session is used for banking information transmitted via an Unsecured Electronic Network. (Article One, subsection 1.7)

Finding: **Compliant**

Recommendations/Concerns

Verified the encryption level of AES 256 bit is applied to ACH records transmitted between the credit unions and CU*Answers via a SOC 1 Report.

Verified the encryption level of RSA 2048 is applied to ACH transactions transmitted through the Bill Pay platform supported by Fiserv via a security certificate on their website.

Verified the encryption level of TLS 1.2 AS 128 bit is applied to ACH transactions transmitted via Magic Wrighter platform based on the security certificate on their website.

Verified MoveIt encryption level of RSA 2048 is applied based on certificate on their website.

8.2E National Association Fees

Verify that for any Entries that are not processed through an ACH Operator but are exchanged with another non-affiliated Participating DFI, the Participating DFI has filed the appropriate N-7 form and paid all Network Administration Fees as required by Section 1.12 (Network Administration fees). (Article One, subsection 1.12)

Finding: **Does Not Apply**

Recommendations/Concerns

8.2F Risk Assessment

Verify that 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.(Article One, subsection 1.2.4)

Finding: **Does Not Apply**

Recommendations/Concerns

Third-Party Processors are not required to conduct an ACH risk assessment.

8.2G Security of Protected Information

Verify that the Participating DFI has established, implemented and updated, as appropriate, security policies, procedures and systems as required by Article One, Section 1.6 (Article One, Section 1.6)

Finding: **Non-Compliant**

Recommendations/Concerns

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. Note:(3) does not apply to CU*Answers

Although policies have been updated to include the ACH Data Security; a self assessment has not been conducted of the initiation, processing, storage and destruction of ACH entries and records.

Note: The destruction of ACH data from the Operations Department is outsourced. This process should be considered during the self-assessment.

Note: The ACH data held by the CUSOs should be included in the self-assessment.

8.3 Audit Requirements for RDFIs

In addition to the audit procedures outlined in Parts 8.1 (General Audit Requirements) and 8.2 (Audit Requirements for All Participating DFIs) of this Appendix Eight, all RDFIs and their Third-Party Service Providers must conduct an audit of the following relating to the receipt of ACH Entries:

8.3A Pre-notifications

Verify that the account number contained in a Prenotification Entry is for a valid account. If the Prenotification does not contain a valid account number, or is otherwise erroneous or unprocessable, verify that the RDFI Transmits either (a) a Return Entry, or (b) a Notification of Change. (Article Three, section 3.5)

Finding: **Does Not Apply**

Recommendations/Concerns

Pre-notifications are included in the daily Exception Report and provided to member credit union's.

8.3B Notifications of Change

Verify that, if the RDFI chooses to initiate Notifications of Change, such COR Entries are Transmitted within two Banking Days of the Settlement Date of the Entry to which the Notification of Change relates, with the exception of Notifications of Change due to merger, acquisition, or other similar events. (Article Three, subsection 3.9.1)

Finding: **Does Not Apply**

Recommendations/Concerns

Notifications of Change are created by member credit unions and transmitted to CU*Answers for further transmission to the Federal Reserve.

8.3C ACH Entries Accepted

Verify that, subject to the RDFI's right of return, all types of Entries that comply with these Rules and are received with respect to an account maintained with the RDFI are accepted. Verify that the RDFI handles XCK Entries and Entries to non-transaction accounts appropriately. (Article Three, subsections 3.1.1 and 3.8.2)

Finding: **Compliant**

Recommendations/Concerns

All valid entries are accepted and posted to the designated account indicated in the ACH entry. Death Notification Entries (DNEs) are provided on a separate report. Reports are available to member credit unions regarding entries subject to Regulation D limitations. International ACH Transactions (IATs) are screened against OFAC prior to posting. IATs that pass the screening are posted by CU*Answers. Suspended IATs are included in the daily exceptions and further due diligence is done by the member credit union. Home equity checks that are converted to ACH are included in the daily exceptions and member credit union decisions the entry.

Unable to test XCK; none found.

8.3D Funds Availability

Verify that, subject to the RDFI's right of return, the amount of each credit Entry received from its ACH Operator is made available to the Receiver for withdrawal no later than the Settlement Date of the Entry. In the case of a credit PPD Entry that is made available to the RDFI by its ACH Operator by 5:00 p.m. (RDFI's local time) on the Banking Day prior to the Settlement Date, verify that the amount is made available to the Receiver for withdrawal at the opening of business on the Settlement Date. Verify that debit Entries are not posted prior to the Settlement Date, even if the Effective Date of the Entry is different from the Settlement Date of the Entry. (Article Three, subsections 3.3.1.1, 3.3.1.2, and 3.3.2)

Finding: **Compliant**

Recommendations/Concerns

Verified ACH credits are posted early morning and debits are scheduled for end of day posting.

8.3E Descriptive Information

For Consumer Accounts, verify that the RDFI provides or makes available to each of its Receivers required information concerning each credit and debit Entry to a Consumer Account of such Receiver. (Article Three, subsection 3.1.5.1) For non-Consumer Accounts, verify that the RDFI provides or makes available to the Receiver the contents of the Check Serial Number Field of an ARC, BOC, or POP Entry. (Article Three, subsection 3.1.5.2)

Finding: **Compliant**

Recommendations/Concerns

Verified the required information is passed to the periodic statement. Verified the Individual ID field is passed for WEB credit entries. Unable to test Machine Transfer Entry (MTE), Shared Network Entry (SHR) and Destroyed Check Entry (XCK); none found.

8.3F, 8.3G, 8.3H Return Entries

Verify that the RDFI Transmits Return Entries to its ACH Operator by the ACH Operator's deposit deadline for the Return Entries to be made available to the ODFI no later than the opening of business on the second Banking Day following the Settlement Date of the original Entry, except as otherwise provided in these Rules. (Article Three, sec tion 3.8) Verify that late returns of unauthorized CCD or CTX Entries are Transmitted with the agreement of the ODFI and that such Entries utilize the appropriate Return Reason Code. (Article Three, subsection 3.8.3.5; Appendix Four) Verify that dishonored Return Entries received by the RDFI are handled appropriately, and that contested dishonored Return Entries and corrected Return Entries are initiated in a timely manner. (Article Three subsection 3.8.5; Appendix Four)

Verify that dishonored Return Entries received by the RDFI are handled appropriately, and that contested dishonored Return Entries and corrected Return Entries are initiated in a timely manner. (Article Three subsection 3.8.5; Appendix Four) Verify that Return Entries relating to RCK Entries are Transmitted to the RDFI's ACH Operator by midnight of the RDFI's second Banking Day following the Banking Day of the receipt of the RCK Entry. (Article Three, subsection3.8.3.3)

Verify that the RDFI returns any credit Entry that is refused by a Receiver by Transmitting a Return Entry to its ACH Operator by the ACH Operator's deposit deadline for the Return Entry to be made available to the ODFI no later than the opening of business on the second Banking Day following the RDFI's receipt of notification from the Receiver that it has refused the Entry. Also verify that the RDFI returns all credit Entries that are not credited or otherwise made available to its Receivers' accounts by Transmitting a Return Entry to its ACH Operator by the ACH Operator's deposit deadline for the Return Entry to be made available to the ODFI no later than the opening of business on the second Banking Day following the Settlement Date of the original Entry. (Article Three, subsections 3.8.3.2 and 3.8.4)

Finding: **Compliant**

Recommendations/Concerns

Verified returns are processed by 3:00 pm daily. Files from member credit unions are batched and upload to FedLine Advantage.
Unable to test dishonored/contested dishonored returns; none found.
Note: Gold platform does not support the dishonored/contested dishonor process. Member credit unions must call CU*Answers staff and the contested dishonored return is processed manually via FedLine Advantage.

Follow-Up: It is noted only one person verifies return totals and transmits file through FedLine. It is recommended dual control be implemented to mitigate operational risk.

8.3I Stop Payment on Consumer Entries

Verify that the RDFI honors stop payment orders provided by Receivers, either verbally or in writing, to the RDFI at least three Banking Days before the scheduled date of any debit Entry to a Consumer Account other than a Single Entry. Verify that the RDFI honors stop payment orders provided by Receivers to the RDFI at such time and in such manner as to allow the RDFI a reasonable opportunity to act upon the order prior to acting on any debit Entry to a non-Consumer Account, or on an ARC, BOC, POP, or RCK Entry or Single Entry IAT, PPD, TEL or WEB Entry to a Consumer Account. Verify that the RDFI is aware that Return Reason Code R08 can be used with any Standard Entry Class Code that carries dollar value. (Article Three, subsections 3.7.1.1, 3.7.1.2 and 3.7.2)

Verify that the RDFI uses Return Reason Codes R38 (Stop Payment on Source Document) and R52 (Stop Payment on Item related to RCK Entry) properly. Verify that, for each ARC, BOC, or RCK Entry for which a stop payment order was in force with respect to (a) the Check that was used as an Eligible Source Document for the ARC or BOC Entry, or (b) the item to which the RCK Entry relates, the Extended Return Entry is Transmitted to the RDFI's ACH Operator by its deposit deadline for the Extended Return Entry to be made available to the ODFI no later than the opening of business on the Banking Day following the sixtieth calendar day following the Settlement Date of the original Entry.
(NOTE: No Written Statement of Unauthorized Debit is required for Entries returned for these reasons.) (Article Three, subsections 3.11.2.2 and 3.13.1; Appendix Four)

Finding: **Does Not Apply**

Recommendations/Concerns

Stop pay orders are handled by member credit unions and not CU*Answers.

8.3J Written Statements of Unauthorized Debits

Verify that Written Statements of Unauthorized Debit are obtained from consumers for all returns bearing Return Reason Codes R05, R07, R10, R37, R51, and R53, and that each Extended Return Entry is Transmitted to the RDFI's ACH Operator by its deposit deadline for the Extended Return Entry to be made available to the ODFI no later than the opening of business on the Banking Day following the sixtieth calendar day following the Settlement Date of the original Entry. Verify that copies of Written Statements of Unauthorized Debits are provided to the ODFI within the required time frame, when such copies are requested in writing by the ODFI. (Article Three subsection 3.11.1, 3.12.5, 3.12.7; and 3.13.1; Appendix Four)

Finding: **Does Not Apply**

Recommendations/Concerns

Written statement requests are handled by member credit unions; not by CU*Answers.

8.3K UCC Article 4A Notice

Verify that the RDFI has provided the Receiver with proper notice to ensure compliance with UCC Article 4A with respect to ACH credit transactions. (Article Three, subsection 3.1.6)

Finding: **Does Not Apply**

Recommendations/Concerns

This is not a requirement of a Third-Party Service Provider.

8.3L CCD, CIE, CTX, IAT Payment Information

Verify that, when requested to do so by the non-Consumer Receiver, the RDFI provides all information contained within the payment-related information field of an Addenda Record(s) Transmitted with a CCD, CTX, CIE, or IAT Entry. The RDFI must provide this information by the opening of business on the RDFI's second Banking Day following the Settlement Date of the Entry. (Article Three, subsection 3.1.5.3)

Finding: **Compliant**

Recommendations/Concerns

Verified addenda is passed to member credit unions. Addenda may be provided electronically via the home banking platform.

THE Payments AUTHORITY
Expect Answers.

2015 ACH Audit Certification

Financial Institution: CU*Answers

Audit Contact: Marsha Sapino

Transit/Routing Number: 6724 6024 3

Date of Audit: September 2-3, 2015

The ACH annual audit was completed in compliance with ACH Operating Rules, Appendix VIII by The Payments Authority.

Auditor: Meg Prieur, AAP

The Payments Authority
580 Kirts Boulevard
Suite 306
Troy, MI 48084