ACH Risk Assessment

September 30, 2019

OVERVIEW

The National Automated Clearing House Association ("NACHA") Article One, Section 1.6 Rule 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 Xtend 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.

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, and current risk trends in the industry. Executive management and the board of directors generally fulfill their duties under the business judgment rule by being aware of risk within Xtend and setting the general risk tolerance of the organization. Xtend 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.

Danielle O'Connor | Xtend, Inc. | Xtend Bookkeeping Manager

ACH LIFE CYCLE DATA FLOW

Xtend performs ACH returns at the request of the credit union.

Daily ACH Files Received

Credit unions receives multiple ACH files throughout the day via FedLine. These files are processed by CU*Answers through its data processing software, CU*BASE GOLD. Files are delivered and posted to credit union client member accounts on the settlement date. The clients choose the frequency of the postings. The ROBOT program gathers all client returns an authorized employee will send the file via FedLine. Xtend will process the return within CU*BASE.

ACH Origination Returns

Credit unions using CU*BASE software receive returns within the ACH files. Xtend's role is to process ACH exceptions per the policies and procedures as agreed between the credit union and Xtend. Xtend will process the ACH Origination Returns by reversing the ACH deposit/credit posted to the members account and providing notification to the credit union.

ACH Dishonored Returns

Credit unions using CU*BASE software receive returns within the ACH files. Xtend's role is to process ACH exceptions per the policies and procedures as agreed between the credit union and Xtend. Xtend will review the dishonored return to determine whether to contest the return back to the Federal Reserve; or process the debit/credit to the member.

Authorized Xtend Employees to Process Exceptions

Three job classifications constitute the authorized members of Xtend to process exceptions. The **Bookkeeping Specialist** is responsible for providing the daily bookkeeping services developed by Xtend SRS for CU*BASE Credit Unions. The **Assistant Manager of Bookkeeping** is responsible for helping the Manager of Bookkeeping perform the daily oversight of the SRS department duties. The **Bookkeeping Services Manager** is responsible for overseeing the Xtend SRS Department. At any given time, there are usually fewer than twenty Xtend employees authorized to process exceptions.

RESPONSE TO AUDIT FINDINGS

The following are Management Responses to the 2019 Fiscal Year ACH Audit:

ARTICLE ONE: GENERAL RULES

Audits of Rules Compliance

Verify the Financial Institution has conducted an audit of compliance with the ACH rules and retained for a period of six years and has obtained certification of completion of an ACH audit from each Third-Party Service Provider.

Finding: Non-Compliant

Xtend has not conducted an audit prior to 2018.

Required Action: To ensure compliance with NACHA rules, Xtend must conduct or have conducted an annual audit of compliance with the Rules. Proof of audit and documentation must be retained for six years.

Management Response:

Fiscal Year 2019 was Xtend's first ACH audit. Management agrees to an ACH audit plan moving forward, where Xtend will perform an internal ACH audit in even-numbered fiscal years and have an external ACH audit performed in odd-numbered fiscal years.

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 DFI, each Non-Consumer Originator and Third- Party Service Provider has implemented policies, procedures and systems to protect the confidentiality and integrity of Protected Information.

Finding: Non-Compliant

To date, Xtend has not conducted an internal assessment related to the security of consumer protected information.
Required Action: To ensure compliance with NACHA Rules, Xtend must establish and implement policies and procedures to conduct a self-assessment that protects the security and integrity of ACH data throughout its life cycle. (NACHA Rule Book, Article One, Section 1.6; OR3) It is noted, Xtend plans to conduct the self-assessment of the security of ACH data by year end.

Management Response:

Xtend shall modify its Cybersecurity Policy to include the following language:

ACH
Xtend shall include as part of this Information Security Program compliance with the NACHA rules regarding "Protected Information," insofar as these rules apply to Xtend. Although Xtend is not a financial institution, Xtend shall protect the confidentiality and integrity or Protected Information; and against unauthorized use of Protected Information that could result in substantial harm to a natural person, as it does with Sensitive Member Data.

Xtend has not conducted an ACH risk assessment.

Recommendation: It is recommended Xtend consider conducting an assessment to identify possible risk associated with ACH processing for multiple Credit Union clients.

Management Response:

This ACH Risk Assessment is designed to place Xtend in compliance with NACHA guidelines. Xtend shall perform an ACH risk assessment annually.

ARTICLE TWO: RIGHTS AND RESPONSIBILITIES OF ODFLS, ORIGINATORS AND THIRD-PARTY SENDERS

Does not apply.

ARTICLE THREE: RIGHTS AND RESPONSIBILITIES OF RDFIS AND THEIR RECEIVERS

Specific Provisions for Exception Processing

Verify that Prenotifications and Notifications of Change are processed appropriately and timely. Verify that all returns, including stop payments, are returned timely and with appropriate return codes and that Written Statements of Unauthorized Debits are obtained from consumers for erroneous transactions.

Finding: Compliant with Exception

Xtend processes daily work for 75 Credit Unions and 30-35 Stand-in Clients. Written procedures are available for Credit Union clients based on individualized Processing Policies.

Pre-notification entries without valid account numbers or transaction codes are reviewed to determine posting, return and/or initiation of Notifications of Change (NOC).

Notifications of Change (NOC) are system generated for Credit Unions that are part of a merge, acquisition or conversion. All other NOC processing is directed by Credit Union individualized Processing Policy.

Xtend takes direction from Credit Union clients to return entries posted after death and upon receipt of a Death Notification Entries (DNE).

Return transactions reviewed in the audit period were returned timely. All return processing, including stop payments and unauthorized entries, are directed by Credit Union individualized Processing Policy.

Exception: During the processing of transactions for one Stand-In client, a non-treasury entry was returned with an incorrect return reason code of R15 - Beneficiary or Account Holder Deceased, with no directive from the client.

Required Action: Xtend must ensure the appropriate return reason code is utilized for return entries as required by NACHA Rules.

Follow-up Action: It is recommended Xtend update procedures to ensure the appropriate use of the R14 - Representative Payee Deceased and R15 - Beneficiary or

Account Holder Deceased return reason codes. ACH Rules intend for the R14 and R15 codes to be used for returning Federal Government benefit payments.

Management Response:

Xtend has updated its ACH Processing Procedures:

Returning Deceased Member Deposits Only for Government Deposits: Xtend will return all government deposit depending on the individual who has passed, such as SSA Treas, US Treas, etc. Xtend will use R14 for Representment payee who is deceased or unable to continue in that capacity. Xtend will use R15 for the Beneficiary or account holder deceased.

Recommendation: Areas of the Processing Policy should be reviewed and updated to ensure compliance with ACH rules and mitigate risk of compliance.

- Pre-notes should be enhanced to include review and action of pre-notification entries.
- Notifications of Change should be addressed separately to explain initiation and dual control.
- Dishonored/Contested Returns need to be defined and appropriately addressed.
- Rejected returns need to be defined and appropriately addressed.
- The process to freeze accounts upon notice of death should be reviewed to ensure appropriate handling of transactions.

Management Response:

Xtend has made the following modifications to Policy:

Pre-notes: Preliminary transactions with an amount equal to zero are sent in advance of the live transactions so that the account number and tran code can be verified. A NOC/notification of change record will be sent back to the originator indicating a change to the account number and/or tran code. Xtend will process NOC for PPD transactions only. The Credit Union can review all prenotes for that day using the PACXTB3 in CU*SPY.

Notifications of Change (NOC): If a transaction requires NOC, Xtend will create a record of change to send back to the originator indicating a recommended update to

the account number and/or tran code. Xtend will process NOC for PPD transactions only.

Dishonored Returns (Rejected): The Federal Reserve will send rejected ACH returns back and they will show on the PACHD2 Dishonored Return/NOC report. An example of these transaction would be anything that was rejected as untimely, field error, etc. Xtend will review these rejected transactions and determine the most appropriate action will be taken based off the reject reason code and the ACH rule book. If a contested return is needed, we will create/build a return on CU*Base using the information/guidance of the ACH rule book and reason code.

Death Notifications: The Federal Reserve will notify us that they received a certificate of death for one of your members by sending us a DNE record where the detail will print on the PACXTB2 report. Xtend will update the ACH record in the ACH distribution maintenance tool #989, so the ACH deposit will kick out to the exceptions when received and we can return that deposit on a timely basis.

Xtend will notify the credit union of any DNE using secured email to send the information over. The credit union will be responsible for updating the member's account number with the date of death and whether or not the account should be frozen.

Recommendation: To ensure consistency among staff, it is recommended Xtend establish and implement a procedure for retention of exception processing directives from Credit Union clients. Consideration should be given to a time frame that provide support in the event of potential disputes.

Management Response:

Xtend has Exception Instructions for staff.

Credit Union Exception Instructions

Department:	Xtend Bookkeeping
Product:	Exception Instructions
Process:	File Retention Audit
Audit Schedule:	Annually

Description: This is to make sure all exception instructions are being stored in the client folders or employee's EOD files.

RISK ASSESSMENT

LIFE CYCLE STAGE: DATA IN TRANSIT TO AND FROM THE FEDERAL RESERVE Governing Policy or Procedures: Xtend ACH Policy

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 (CU*BASE)*	*The likelihood that our encryption level could be cracked*	**MODERATE (DUE TO HIGH IMPACT OF THE EVENT)**
*Communication lines between the Fed and CU*BASE (CU*Answers) are damaged for an extended period of time*	**LOW**	*Tested annually through the CU*Answers DR/BR with gap analysis available to Xtend* *If CU*BASE is unavailable, Xtend will prepare for missing deadlines and what that impact would be on the credit union* *Xtend would submit share draft returns manually through the credit unions share draft vendor website if needed*	*Xtend unable to process in a timely manner*	**LOW**

LIFE CYCLE STAGE: DATA AT REST

Governing Policy or Procedures: Information Security Program/Cybersecurity Program

INHERENT RISKS	RISK RATING	CONTROLS	RESIDUAL RISKS	RESIDUAL RATING
Malicious hacks into our network	**HIGH**	*Xtend's networks and data hosting is managed by CU*Answers and those controls are described in CU*Answers' annual SSAE-18 reports*	*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)**
Unauthorized access to ACH information	**HIGH**	*Library software allows financial institutions to control*	*Theft of information*	**MODERATE (DUE TO HIGH IMPACT OF THE EVENT)**

		who can see and access reports *Xtend performs quarterly access audits*		
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

No applicable risks (backups are provided for on CU*Answers ACH Audit)

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**