

Center Parc Credit Union

## ACH ORIGATION PRODUCT SCHEDULE

By signing this ACH Origination Product Schedule ("Product Schedule") You ("Member") hereby requests Center Parc Credit Union (Center Parc) ("Financial Institution") to provide the Services described in this Product Schedule, and Member accepts and agrees to all terms, conditions, and provisions of this Product Schedule and agrees that this Product Schedule sets forth the terms and conditions pursuant to which Financial Institution will provide to Member the ACH Services outlined herein ("Services"). Member further agrees that this Product Schedule is entered into as a Product Schedule under the Business Online Banking and Master Cash Management Agreement ("Master Agreement"). Financial Institution and Member agree that by executing this Product Schedule, Member acknowledges receipt of and agrees to the terms of the Master Agreement.

Member wishes to initiate credit and/or debit Entries through the Financial Institution to accounts maintained at Financial Institution and in other depository financial institutions by means of the Automated Clearing House Network ("ACH") pursuant to the terms of this Product Schedule and the rules of the National Automated Clearing House Association ("NACHA") and Financial Institution's operating rules and procedures for electronic entries, including any exhibits or appendices thereto now in effect, or as may be amended from time to time, (the "Rules"), and Financial Institution is willing to act as an Originating Depository Financial Institution ("ODFI") with respect to such Entries. In the event of inconsistency between a provision of this Product Schedule, the Uniform Commercial Code ("UCC"), the Master Agreement, and/or the Depository Agreement, the provisions of this Product Schedule shall prevail. Terms not otherwise defined in this Product Schedule shall have the meaning ascribed to those terms in the Rules. The term "Entry" shall have the meaning provided in the Rules and shall also mean the data received from Member hereunder from which Financial Institution initiates each Entry.

Therefore, in consideration of the mutual promises contained herein and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, Financial Institution and Member, intending to be legally bound, do hereby agree as follows:

### AGREEMENT

- 1. COMPLIANCE WITH RULES AND LAWS.** Member acknowledges it has a copy or has access to a copy of the Rules. The Rules may also be purchased online at [www.nacha.org](http://www.nacha.org) under the publications tab. Member agrees to comply with and be subject to the Rules of NACHA in existence at the date of this Product Schedule, and any amendments to these Rules made from time to time. It shall be the responsibility of the Member that the origination of ACH transactions complies with U.S. law, including but is not limited to sanctions enforced by the Office of Foreign Assets Control ("OFAC"). It shall further be the responsibility of the Member to obtain information regarding such OFAC enforced sanctions. (This information may be obtained directly from the OFAC Compliance Hotline at 800- 540-OFAC or from the OFAC's home page site at [www.ustreas.gov/ofac](http://www.ustreas.gov/ofac). Member agrees that the performance of any action by Financial Institution to debit or credit an account or transfer funds otherwise required by the Rules is excused from the performance of such action to the extent that the action is inconsistent with United States law, including the obligations of the Financial Institution under OFAC or any program administered by the United States Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"). Member agrees generally and warrants to Financial Institution that all actions by Member contemplated by this Product Schedule, including the preparation, transmittal, and settlement of Entries and payment orders, shall comply in all material respects with United States laws, regulations, regulatory guidelines and guidance, and official commentaries, including without limitation all such regulations, guidelines, and commentaries issued by the Board of Governors of the Federal Reserve and the Federal Financial Institutions Examination Council ("FFIEC"). Financial Institution will charge the Member with any fines or penalties imposed by OFAC, NACHA or any organization which are incurred as a result of non-compliance by the Member and the Member agrees to fully reimburse and/or indemnify Financial Institution for such charges or fines. The specific duties of the Member provided in the following paragraphs of this Product Schedule in no way limit the foregoing undertaking. The duties of the Member set forth in the following paragraphs of this Product Schedule in no way limit the requirement of complying with the Rules.

2. **UNDERWRITING.** Member approval for use of this Service may be subject to underwriting criteria established by Financial Institution from time to time. If Financial Institution requires application of underwriting criteria to Member approval for use of this Service, Financial Institution will communicate to Member the nature and content of that criteria and the information Member will be required to provide to Financial Institution. Member agrees to provide Financial Institution such financial, business and operating information as Financial Institution may reasonably request in connection with Financial Institution's underwriting and approval process.
3. **SECURITY INTEREST.** To secure the payment and performance of Member's obligations set forth herein, Member grants to Financial Institution a security interest in and pledges and assigns to Financial Institution all of Member's right, title, and interest in the following described property, whether now owned or hereafter existing or acquired and wherever located: (a) all monies, instruments, savings, checking and other accounts of Member (excluding IRA, Keogh, trust accounts and other accounts subject to tax penalties if so assigned) that are now or in the future in Financial Institution's custody or control; (b) any other collateral described in any security instrument securing the obligations of Member to Financial Institution under this Product Schedule or any other obligation of Member to Financial Institution; and (c) all proceeds and products of the property as well as any replacements, accessions, substitutions, and additions to any of the above.
4. **DESIGNATION OF ADMINISTRATOR.** In order to originate ACH Entries, Member must designate at least one Administrator. Administrator(s) shall be responsible for designating "Users" who Member authorizes to issue Entries on its behalf. For the purposes of this Product Schedule, the term User shall also include the Administrator. The Financial Institution shall be entitled to rely on the designations made by the Member's Administrator(s) and shall not be responsible for matching the names of the Member Users designated by the Administrator(s) to names or titles listed in Member's banking resolutions. Member agrees that any such online Entries shall comply with Financial Institution's Security Procedures, which are subject to change without notice to Member. Although Financial Institution is only required to act upon the instructions of the User(s), the Financial Institution may, in its sole discretion, execute debit or credit Entries initiated by any individuals authorized by Member to sign checks on Member accounts. The signature cards establishing the authorized signatories for Member deposit accounts are hereby incorporated by reference and made a part hereof.
5. **TRANSMISSION OF ENTRIES BY MEMBER.** User(s) shall initiate the debit or credit Entries in **Schedule A** hereunder on behalf of and selected by Member. Financial Institution shall be entitled to deem any person having knowledge of any Security Procedure, defined below in Section 8 of this Product Schedule and required to initiate Entries under this Product Schedule, to be a User. User(s) shall transmit Entries to Financial Institution in computer readable form in compliance with the formatting and other requirements set forth in the NACHA file specifications or as otherwise specified by Financial Institution. Entries shall be transmitted to Financial Institution no later than the time and the number of days prior to the Effective Entry Date specified in **Schedule A**. For the purposes of this Product Schedule, "Business Day" means Monday through Friday, excluding federal holidays and the "Settlement Date" with respect to any Entry shall be the Business Day when such Entry is debited or credited in accordance with the Rules. A federal holiday calendar can be found in **Schedule A**. Entries received after the cut-off time shall be deemed to have been received on the next Business Day. The total dollar amount of Entries transmitted by Member to Financial Institution on any one Business Day shall not exceed the lesser of the amount of collected funds in Member's account or the established ACH Limits. Member may not reinitiate entries except as prescribed by the Rules.

"Entry Settlement Limit" means the maximum aggregate amount of In-Process Entries permitted to be outstanding at any time, which amount shall be separately communicated to Member by Financial Institution in writing from time to time.

"In-Process Entries" means the aggregate dollar amount of all credit or debit Entries initiated by Member and in process on any date for which settlement has not occurred with respect to credit Entries, or the applicable period for the return of items has not expired with respect to debit Entries.

"Overlimit Entry" means an Entry the amount of which would cause the aggregate amount of In-Process Entries to exceed the Entry Settlement Limit. Member agrees that Financial Institution will not process an Overlimit Entry. Financial Institution will suspend any Overlimit Entry submitted by Member and may, following its receipt of an Overlimit Entry; suspend all In-Process Entries. Member acknowledges that any Overlimit Entry or other In-Process

Entries suspended by Financial Institution will not settle on their scheduled Settlement Date. If Member wishes to initiate an Entry that would cause the amount of In-Process Entries to exceed the Entry Settlement Limit, Member may submit to Financial Institution its request to initiate an Entry that otherwise would be an Overlimit Entry. Member must submit its request at least 2 banking days prior to the date on which Member wishes to initiate the Entry that otherwise would be an Overlimit Entry. Financial Institution may require from Member financial or other information in connection with Financial Institution's consideration of the request. Financial Institution may grant or deny Member's request at its sole discretion. In addition to the foregoing, Financial Institution generally reserves the right to limit the nature and amount of the preauthorized debit/credit Entries processed under this Product Schedule or to refuse to process any debit/credit Entries under this Product Schedule if, in Financial Institution's sole judgment (i) there is reasonable cause to believe that any Entry will be returned or will not settle in the ordinary course of the transaction for any reason, (ii) to do otherwise would violate any limit set by the applicable clearing house association or any governmental authority or agency to control payment system risk, or (iii) a preauthorized credit Entry or the return of a preauthorized debit Entry would create an overdraft of Member's Accounts. If any of the foregoing actions are taken by Financial Institution with respect to a particular preauthorized debit/credit Entry, Financial Institution will notify Member as promptly as practicable, but in no event later than 2 banking days after its decision. Member may not reinitiate entries except as prescribed by the Rules.

6. **THIRD-PARTY SERVICE PROVIDERS.** Member may be using special equipment, services or software provided by a third party to assist it in processing Files hereunder ("Service Provider"). Member agrees not to use a Service Provider to transmit files to Financial Institution without first entering into Financial Institution's Third-Party Service Provider Agreement. If Member uses Service Provider to transmit Files to Financial Institution and Member and Service Provider have not entered into a Third-Party Service Provider Agreement, Member (a) agrees that Service Provider is acting as Member's agent in the delivery of Files to Financial Institution, and (b) agrees to assume full responsibility and liability for any failure of Service Provider to comply with the laws of the United States, the Rules and this Product Schedule. Financial Institution will not be liable for any losses or additional costs incurred by Member as a result of any error by Service Provider or a malfunction of equipment provided by Service Provider. Member is solely responsible for maintaining compliance with the requirements of Service Provider, including obtaining any software updates. Financial Institution's sole responsibility shall be to transmit Financial Institution approved transactions to the ACH Operator and Financial Institution shall not have any responsibility for any File handled by Service Provider until that point in time when Financial Institution accepts and approves a File from such Service Provider for processing. If Financial Institution authorizes Member to use a Service Provider, the terms and conditions governing the relationship between Member and the Service Provider shall be governed by a separate agreement between Member and Service Provider ("Service Provider Agreement"). All of Member's obligations and responsibilities under this Product Schedule will apply to the Service Provider, and Member's separate agreement with the Service Provider must so provide. At Financial Institution's request, Member will provide to Financial Institution a true and exact copy of such agreement. Member shall designate the Service Provider as a User and the Service Provider must also enter into a Service Provider Agreement before the Service Provider sends Files to Financial Institution. Notwithstanding the foregoing, Member hereby authorizes Financial Institution to accept any File submitted by the Service Provider even if the Service Provider has not been designated as a User or if the Third-Party Service Provider has not executed the Service Provider Agreement. Member hereby indemnifies and holds Financial Institution harmless for any losses, damages, fines, assessments, costs and expenses incurred or suffered by Financial Institution or any other person as a result of or arising from Member's use of Service Provider, including fines or assessments incurred under or pursuant to the Rules and attorneys' fees.
7. **SECURITY PROCEDURES.** In addition to, and without limiting the generality of, the Security Procedure provisions of the Master Agreement, the Member shall comply with the Security Procedures below. Your Business Wire (online banking) and ACH entry protection is important to us. Because of this importance, Center Parc offers numerous security procedures to protect your online banking and ACH transfers, especially given the current levels of online banking fraud. You and your business understand and agree that the authenticity of any ACH transaction or Wire transmitted to Center Parc will be verified pursuant to the following security procedures.

**SECURITY PROCEDURES:**

- a) **Dual Control** - Two employees or authorized individuals must approve an ACH transfer or wire.
- b) **Dedicated Computer**- Your company designates a computer or authorized device used exclusively for conducting financial transactions with limited access and restricted non-financial use.
- c) **Payment Activity Review**- Center Parc will monitor the Wire and ACH transactions to determine whether they are consistent with the normal course and scope of your business activity.

- d) **Daily Transfer Limits-** Center Parc will limit the amount of funds your business can transfer by wire or ACH based on approved limits requested in this application. Additionally, your business may establish internal limits for employees who draft or approve ACH or Wire transfers.
- e) **Soft tokens-** A software-based security token and technique providing two factor authentication via a passcode or PIN to authorize transactions or system access.
- f) **E-Mail verification-** Center Parc will send designated individuals an email confirming that a wire or ACH has been initiated and requesting verification of the legitimacy of the transfer.
- g) **Process Calendar** – Limits the dates and times when wire and ACH transfers can occur.
- h) **Malware Protection Software** – Center Parc warrants that the business has up to date antivirus/malware protection installed and functioning on any device used for financial transactions.

If the Business fails to meet these Security Procedures, the Business acknowledges that Center Parc first offered security procedures that reflect risk-based processes and procedures reasonably intended to identify fraudulent entries, consistent with applicable NACHA requirements. The Business assumes responsibility for any resulting risk. The Business further warrants that it waives its ability to bring suit against Center Parc for violations of Article 4A of the Uniform Commercial Code. By failing to adopt these risk-based Security Procedures, the Business agrees to hold Center Parc harmless for any erroneous or fraudulent wire or ACH transfers. Additionally, Center Parc may refuse to accept any request for wire or ACH transfers initiated by the Business and may discontinue services should the Business reject these Security Procedures.

- 8. **PHYSICAL AND ELECTRONIC SECURITY.** In addition to, and without limiting the generality of, the Physical and Electronic Security provisions of the Master Agreement, Member specifically acknowledges and agrees that as part of its obligation to provide for the security of data and systems in Member's possession or under Member's control, Member shall comply with the provisions of Section 1.6 of the Rules, entitled "Security Requirements," for the safeguarding of Protected Information, as that term is defined in the Rules.
- 9. **INTERNATIONAL ACH TRANSACTIONS ("IAT").** Member shall not initiate any IAT Entries without Financial Institution's prior approval. If approved by Financial Institution, the following provisions apply to IAT Entries originated by Company:
  - a) IAT Entries are transmitted by Financial Institution in U.S. dollars and converted to the local currency for receipt in the foreign country at the exchange rate determined by Financial Institution's processor on the date determined by Financial Institution's processor. All risk of fluctuation in the applicable exchange rate is borne by Member and Member agrees and acknowledges that Financial Institution shall not be liable to Member for any loss or charge incurred by Member as the result of the application of any foreign currency exchange criteria imposed by any institution or agency located outside the United States.
  - b) In the event of a returned IAT Entry, consumer payments will be credited to Member at the originated U.S. dollar amount; corporate payments will be credited to Member at the exchange rate determined by Financial Institution's processor at the time of return.
  - c) In the event of an error in an Entry or duplicate entries, Member acknowledges and agrees that Member shall be liable for any and all losses caused by and a direct or indirect result from the error or duplicate Entry.
  - d) Member shall originate all International ACH Transactions, as that term is defined in the Rules, with an IAT SEC code and Member hereby agrees to abide by all of the Rules related to IAT Entries.
  - e) Member agrees that in the case of a non-Consumer Account, Member shall enter into an agreement with the Receiver whereby the Receiver agrees to abide by the Rules in effect from time to time.
  - f) Member acknowledges that it has reviewed and understands the section of the Rules entitled (or otherwise dealing with) "Rules Exceptions for Outbound IAT Entries" and Member understands and agrees that laws, regulations, and rules of the country in which the Receiver is located shall govern the matters listed within that subsection. Member further acknowledges that Member understands how such laws, regulations and rules differ from the Rules.
  - g) Member hereby indemnifies Financial Institution from and against any and all resulting claims, demands, losses, liabilities, or expenses, including attorneys' fees and costs, resulting directly or indirectly from Member's origination of an IAT Entry.
  - h) Member agrees and acknowledges that any assistance by Financial Institution does not in any manner obligate Financial Institution for the accuracy or enforceability of the Entry in any country outside the United States.
  - i) Member bears the risk of any loss caused by any delay, tax, cost, tariff, fee, or other charge incurred on account of the Entry in any country outside the United States.

- j) If the settlement of any IAT Entry involves clearing of the Entry in more than one country outside the United States, Financial Institution shall be permitted to rely upon any advice or instruction received by Financial Institution from the financial institution or financial agency located in the first country outside the United States to which the Entry is directed.
- k) IAT Entries must be authorized as provided in the Rules. The form and content of the authorization, including whether such authorization may be oral, electronic, or written, shall be governed by the laws and payment system rules of the receiving country.
10. **CREDIT AND DEBIT ENTRIES; RECORDS RETENTION.** Member shall obtain an authorization (“Authorization Agreement”) as required by the Rules from the person or entity whose account will be debited or credited as the result of a debit or credit Entry initiated by Member and Member shall retain the Authorization Agreement in original form while it is in effect and the original or a copy of each authorization for three (3) years after termination or revocation of such authorization as stated in the Rules. Upon request, Member shall furnish the original or a copy of the authorization to any affected Participating Depository Financial Institution, as defined in the Rules. Financial institution agrees to provide the identity of affected Participating Depository Financial Institutions to Member upon written request by Member. Member shall be solely responsible for communicating with the Participating Depository Financial Institution to establish the method by which the Authorization Agreement will be provided and Member agrees to provide the Authorization Agreement to the identified Participating Depository Financial Institution within the time frame identified in the Rules.
- Member shall ensure that all authorization requirements of the Rules for each SEC Code are satisfied and in compliance with the Rules.
11. **RECORDING AND USE OF COMMUNICATIONS.** Member and Financial Institution agree that all telephone conversations or data transmissions between them or their agents made in connection with this Product Schedule may be electronically recorded and retained by either party by use of any reasonable means. Financial Institution shall not be obligated to make such recordings.
12. **PROCESSING, TRANSMITTAL, AND SETTLEMENT BY FINANCIAL INSTITUTION.** Except as otherwise provided for in this Product Schedule and if Financial Institution elects to accept Entries, Financial Institution shall:
- a) (i) use commercially reasonable efforts to comply with the instructions of Member, (ii) process Entries received from Member to conform with the file specifications set forth in the Rules, (iii) transmit such Entries as an ODFI to the "ACH" processor selected by Financial Institution, (iv) settle for such Entries as provided in the Rules, and (v) in the case of a credit Entry received for credit to an account with Financial Institution ("On-Us Entry"), Financial Institution shall credit the Receiver's account in the amount of such credit Entry on the Effective Entry Date contained in such credit Entry provided such credit Entry is received by Financial Institution at the time and in the form prescribed by Financial Institution in Section 5.
- b) transmit such Entries to the ACH processor by the deposit deadline of the ACH processor, provided: (i) such Entries are completely received by Financial Institution's cut-off time at the location specified by Financial Institution to Member from time to time; (ii) the Effective Entry Date satisfies the criteria provided by Financial Institution to Member; and (iii) the ACH processor is open for business on such Business Day. Member agrees that the ACH processor selected by Financial Institution shall be considered to have been selected by and designated by Member. The Member will receive immediately available funds for any electronic debit entry initiated by it on the Settlement Date applicable thereto.
13. **PAYMENT FOR CREDIT ENTRIES AND RETURNED DEBIT ENTRIES.** Member agrees to pay for all credit Entries issued by Member, User(s), or credit Entries otherwise made effective against Member. Member shall make payment to Financial Institution on the date as determined by Financial Institution in its sole discretion, (“Payment Date”). Member shall pay Financial Institution for the amount of each debit Entry returned by a Receiving Depository Financial Institution (“RDFI”) or debit Entry dishonored by Financial Institution. Payment shall be made by Member to Financial Institution in any manner specified by Financial Institution. Notwithstanding the foregoing, Financial Institution is hereby authorized to charge the account(s) ("Authorized Account(s)") designated on the Business Online Banking Cash Management Application, as payment for all payments due Financial Institution under this Agreement. Member shall maintain sufficient collected funds in the Authorized Account(s) to pay for all payments due Financial Institution under this Agreement on the Payment Date. In the event the Authorized Account or any other Member credit union account does not have collected funds sufficient on the Payment Date to cover the total amount of all Entries to be paid on such Payment Date,

Financial Institution may take any of the following actions:

- a) Refuse to process all Entries, in which event Financial Institution shall return the data relating to such credit Entries to Member, whereupon Financial Institution shall have no liability to Member or to any third party as a result thereof; or
  - b) Process that portion of the credit Entries as Member has sufficient available funds in the Authorized Account to cover, in whatever order Financial Institution in its sole discretion shall elect to process, in which event Financial Institution shall return the data relating to such credit Entries as are not processed to Member, whereupon Financial Institution shall have no liability to Member or any third party as a result thereof; or
  - c) Process all credit Entries. In the event Financial Institution elects to process credit Entries initiated by Member and Member has not maintained sufficient available funds in the Authorized Account with Financial Institution to cover them, the total amount of the insufficiency advanced by Financial Institution on behalf of Member shall be immediately due and payable by Member to Financial Institution without any further demand from Financial Institution. If Financial Institution elects to pay Member's account in the overdraft on any one or more occasions, it shall not be considered a waiver of Financial Institution's rights to refuse to do so at any other time nor shall it be an agreement by Financial Institution to pay other items in the overdraft.
14. **PRE-FUNDING.** Financial Institution reserves the right to require Member to pre-fund an Account maintained at Financial Institution prior to the Settlement Date of the ACH file. Financial Institution shall determine whether pre-funding is required based on criteria established from time to time by Financial Institution. Financial Institution will communicate directly to Member if pre-funding is required and, if requested by Member, will provide Member with an explanation of its pre-funding criteria. If it is determined that pre-funding is required, Member will provide immediately available and collected funds sufficient to pay all Entries initiated by Member (a) not later than 8:30 a.m. local time 3 banking days before each Settlement Date, and (b) prior to initiating any Entries for which pre-funding is required.
15. **ON-US ENTRIES.** Except as provided in Section 17, Rejection of Entries, or in the case of an Entry received for credit to an account maintained with Financial Institution (an "On-Us Entry"), the Financial Institution shall credit the Receiver's account in the amount of such Entry on the Effective Entry Date contained in such Entry, provided the requirements set forth in Section 12 (b) (i), (ii), and (iii) are met. If any of those requirements are not met, the Financial Institution shall use reasonable efforts to credit the Receiver's account in the amount of such Entry no later than the next Business Day following such Effective Entry Date.
16. **RESERVES.** From time to time, Financial Institution shall evaluate Member's transaction activity for the purpose of establishing averages for transaction frequency, amount, returns and adjustments. These evaluations will occur at least annually and may occur more frequently at Financial Institution's discretion. In connection with these evaluations, Financial Institution reserves the right to require Member to establish reserves with Financial Institution calculated by Financial Institution to cover Member's obligations to Financial Institution arising from ACH activities under this Product Schedule. Reserves may be expressed as a fixed dollar amount or as a "rolling reserve" calculated based on "rolling" averages determined by Financial Institution's periodic evaluations. The amount of reserves required by Financial Institution, if any, will be communicated directly to Member from time to time. Member agrees to establish reserves as required by Financial Institution within 10 banking days after receipt of a communication from Financial Institution setting forth the amount of required reserves and the basis of calculation used to determine the amount of reserves. Financial Institution may suspend ACH processing activity for Member if Member fails to establish the required amount of reserves within the time period specified by Financial Institution in its communication to Member.
17. **REJECTION OF ENTRIES.** Member agrees that Financial Institution has no obligation to accept Entries and therefore may reject any Entry issued by Member. Financial Institution has no obligation to notify Member of the rejection of an Entry but Financial Institution may do so at its option. Financial Institution shall have no liability to Member for rejection of an Entry and shall not be liable to pay interest to Member even if the amount of Member's payment order is fully covered by a withdrawable credit balance in an Authorized Account of Member or the Financial Institution has otherwise received full payment from Member.
18. **CANCELLATION OR AMENDMENT BY MEMBER.** Member shall have no right to cancel or amend any Entry after its receipt by Financial Institution. However, Financial Institution may, at its option, accept a cancellation or amendment by Member. If Financial Institution accepts a cancellation or amendment of an Entry, Member must comply with the Security Procedures provided in Section 6 of this Product Schedule. If such a request is received by the Financial Institution before the affected Entry has been transmitted to the ACH (or, in the case of an On-Us

Entry, before the Receiver's account has been credited or debited), the Financial Institution will use reasonable efforts to cancel or amend the Entry as requested, but the Financial Institution shall have no liability if the cancellation or amendment is not affected. If Financial Institution accepts a cancellation or amendment of an Entry, Member hereby agrees to indemnify, defend all claims and hold Financial Institution harmless from any loss, damages, or expenses, including but not limited to attorney's fees, incurred by Financial Institution as the result of its acceptance of the cancellation or amendment.

**19. REVERSALS OF ENTRIES.**

- a) **General Procedure.** Upon proper and timely request by the Member, the Financial Institution will use reasonable efforts to affect a reversal of an Entry or File to the extent reversal is expressly permitted by the Rules. To be "proper and timely," the request must (i) be made within five (5) Business Days of the Effective Entry Date for the Entry or File to be reversed; (ii) be made immediately, not to exceed ten (10) hours, upon discovery of the error; (iii) be accompanied by a Reversal/Cancellation Request form, and (iv) the basis for such reversal must be expressly permitted by the Rules and otherwise in compliance with the Rules. In addition, if the Member requests reversal of a Debit Entry or Debit File, it shall concurrently deposit into the Member Account an amount equal to that Entry or File. The Member shall notify the Receiver of any reversing Entry initiated to correct any Entry it has initiated in error. The notification to the Receiver must include the reason for the reversal and be made no later than the Settlement Date of the reversing Entry.
- b) **No Liability: Reimbursement to the Financial Institution.** Under no circumstances shall the Financial Institution be liable for interest or related losses if the requested reversal of an Entry is not effected. The Member shall reimburse the Financial Institution for any expenses, losses or damages it incurs in effecting or attempting to affect the Member's request for reversal of an Entry.

**20. ERROR DETECTION.** Financial Institution has no obligation to discover and shall not be liable to Member for errors made by Member, including but not limited to errors made in identifying the Receiver, or an Intermediary or RDFI or for errors in the amount of an Entry or for errors in Settlement Dates. Financial Institution shall likewise have no duty to discover and shall not be liable for duplicate Entries issued by Member.

Notwithstanding the foregoing, if the Member discovers that any Entry it has initiated was in error, it shall notify the Financial Institution of such error. If such notice is received no later than four (4) hours prior to the ACH processing deadline, the Financial Institution will utilize reasonable efforts to initiate an adjusting Entry or stop payment of any On-Us" credit Entry within the time limits provided by the Rules. In the event that Member makes an error or issues a duplicate Entry, Member shall indemnify, defend all claims, and hold Financial Institution harmless from any loss, damages, or expenses, including but not limited to attorney's fees, incurred by Financial Institution as result of the error or issuance of duplicate Entries.

**21. PROHIBITED TRANSACTIONS.** Member agrees not to use or attempt to use the Services (a) to engage in any illegal purpose or activity or to violate any applicable law, rule or regulation, (b) to breach any contract or agreement by which Member is bound, (c) to engage in any internet or online gambling transaction, whether or not gambling is legal in any applicable jurisdiction, or (d) to engage in any transaction or activity that is not specifically authorized and permitted by this Agreement. Member acknowledges and agrees that Financial Institution has no obligation to monitor Member's use of the Services for transactions and activity that is impermissible or prohibited under the terms of this Agreement; provided, however, that Financial Institution reserves the right to decline to execute any transaction or activity that Financial Institution believes violates the terms of this Agreement.

**22. PRENOTIFICATION.** Member, at its option, may send prenotification that it intends to initiate an Entry or Entries to a particular account within the time limits prescribed for such notice in the Rules. Such notice shall be provided to the Financial Institution in the format and on the medium provided in the media format section of such Rules. If Member receives notice that such prenotification has been rejected by an RDFI within the prescribed period, or that an RDFI will not receive Entries without having first received a copy of the Authorization signed by its member, Member will not initiate any corresponding Entries to such accounts until the cause for rejection has been corrected or until providing the RDFI with such authorization within the time limits provided by the Rules.

**23. NOTICE OF RETURNED ENTRIES AND NOTIFICATIONS OF CHANGE.** Financial Institution may notify Member by e-mail, facsimile transmission, US mail, or other means of the receipt of a returned Entry from the ACH

Operator. Except for an Entry retransmitted by Member in accordance with the requirements of Section 5, Financial Institution shall have no obligation to retransmit a returned Entry to the ACH Operator if Financial Institution complied with the terms of this Product Schedule with respect to the original Entry. Member shall notify the Receiver by phone or electronic transmission of receipt of each return Entry no later than one Business Day after the Business Day of receiving such notification from Financial Institution. Financial Institution shall provide Member all information, as required by the Rules, with respect to each Notification of Change (“NOC”) Entry or Corrected Notification of Change (“Corrected NOC”) Entry received by Financial Institution relating to Entries transmitted by Member. Financial Institution must provide such information to Member within two (2) banking days of the Settlement Date of each NOC or Corrected NOC Entry. Member shall ensure that changes requested by the NOC or Corrected NOC are made within six (6) banking days of Member's receipt of the NOC information from Financial Institution or prior to initiating another Entry to the Receiver's account, whichever is later.

24. **ACCOUNT RECONCILIATION.** The Member agrees to notify the Financial Institution promptly of any discrepancy between the Member's records and the information shown on any periodic statement. If the Member fails to notify the Financial Institution within ten (10) calendar days of receipt of a periodic statement containing such information; the Member agrees that the Financial Institution shall not be liable for any other losses resulting from the Member's failure to give such notice or any loss of interest or any interest equivalent with respect to any Entry shown on such periodic statement. If the Member fails to notify the Financial Institution within thirty (30) calendar days of receipt of such periodic statement, the Member shall be precluded from asserting any discrepancy against the Financial Institution.
25. **PROVISIONAL SETTLEMENT.** Member shall be bound by and comply with the Rules as in effect from time to time, including without limitation the provision thereof making payment of an Entry by the RDFI to the Receiver provisional until receipt by the RDFI of final settlement for such Entry; and Member acknowledges that it has received notice of that Rule and or the fact that, if such settlement is not received, the RDFI shall be entitled to a refund from the Receiver of the amount credited and Member shall not be deemed to have paid the Receiver the amount of the Entry.
26. **MEMBER REPRESENTATIONS AND WARRANTIES; INDEMNITY.** With respect to each and every Entry transmitted by Member, Member represents and warrants to Financial Institution and agrees that (a) each person or entity shown as the Receiver on an Entry received by Financial Institution from Member has authorized the initiation of such Entry and the crediting or debiting of its account in the amount and on the Effective Entry Date shown on such Entry, (b) such authorization is operative at the time of transmittal or crediting or debiting by Financial Institution as provided herein, (c) Entries transmitted to Financial Institution by Member are limited to those types of credit and debit Entries set forth in **Schedule A**, (d) Member shall perform its obligations under this Product Schedule in accordance with all applicable laws, regulations, and orders, including, but not limited to, the sanctions laws, regulations, and orders administered by OFAC; laws, regulations, and orders administered FinCEN; and any state laws, regulations, or orders applicable to the providers of ACH payment services, (e) Member shall be bound by and comply with the provision of the *Rules* (among other provisions of the *Rules*) making payment of an Entry by the RDFI to the Receiver provisional until receipt by the RDFI of final settlement for such Entry; and (f) Member shall ensure that any and all non-public personal information provided by Member to Financial Institution shall be secure and will not be disclosed to any unauthorized person. Member specifically acknowledges that it has received notice of the rule regarding provisional payment and of the fact that, if such settlement is not received, the RDFI shall be entitled to a refund from the Receiver of the amount credited and Member shall not be deemed to have paid the Receiver the amount of the Entry. The Member shall defend, indemnify, and hold harmless the Financial Institution, and its officers, directors, agents, and employees, from and against any and all actions, costs, claims, losses, damages, or expenses, including attorney's fees and expenses, resulting from or arising out of (aa) any breach of any of the agreements, representations or warranties of the Member contained in this Product Schedule; or (bb) any act or omission of the Member or any other person acting on the Member's behalf.
27. **ADDITIONAL MEMBER WARRANTIES FOR SELECTED STANDARD ENTRY CLASSES.** NACHA, in its role of ensuring the safety, security, and viability of the ACH network, has determined that certain single-use or limited-use consumer authorizations have the potential to increase risk in the ACH system and compromise system effectiveness by increasing the incidence of returned Entries. Therefore, to qualify

as an Originator of such Entries, Member hereby warrants to Financial Institution that for each such ACH Entry submitted for processing, Member has obtained all authorizations from the Receiver as required by the Rules, by Regulation E or other applicable law, and this Product Schedule. Member also makes the additional warranties to Credit Union that Credit Union makes to each RDFI and ACH Operator under the Rules for the respective SEC codes for Entries originated by Member. Member hereby indemnifies and holds Financial Institution harmless from any liability arising out of Member's breach of these warranties.

28. **FINANCIAL INFORMATION AND AUDIT.** Financial Institution may from time-to-time request information from Member in order to evaluate a continuation of the Service to be provided by Financial Institution hereunder and/or adjustment of any limits set by this Product Schedule. Member agrees to provide the requested financial information immediately upon request by Financial Institution, in the form required by Financial Institution. Member authorizes Financial Institution to investigate or reinvestigate at any time any information provided by Member in connection with this Product Schedule or the Service. Upon request by Financial Institution, Member hereby authorizes Financial Institution to enter Member's business premises for the purpose of ensuring that Member is in compliance with this Product Schedule and Member specifically authorizes Financial Institution to perform an audit of Member's operational controls, risk management practices, staffing and the need for training and ongoing support, and information technology infrastructure. Member hereby acknowledges and agrees that Financial Institution shall have the right to mandate specific internal controls at Member's location(s) and Member shall comply with any such mandate. In addition, Member hereby agrees to allow Financial Institution to review available reports of independent audits performed at the Member location related to information technology, the Service and any associated operational processes. Member agrees that if requested by Financial Institution, Member will complete a self-assessment of Member's operations, management, staff, systems, internal controls, training and risk management practices that would otherwise be reviewed by Financial Institution in an audit of Member. If Member refuses to provide the requested financial information, or if Financial Institution concludes, in its sole discretion, that the risk of Member is unacceptable, if Member violates this Product Schedule or the Rules, or if Member refuses to give Financial Institution access to Member's premises, Financial Institution may terminate the Service and this Product Schedule according to the provisions hereof.

**29. LIMITATION OF LIABILITY.**

- a) IN THE PERFORMANCE OF THE SERVICES REQUIRED BY THIS AGREEMENT, FINANCIAL INSTITUTION SHALL BE ENTITLED TO RELY SOLELY ON THE INFORMATION, REPRESENTATIONS, AND WARRANTIES PROVIDED BY MEMBER PURSUANT TO THIS AGREEMENT, AND SHALL NOT BE RESPONSIBLE FOR THE ACCURACY OR COMPLETENESS THEREOF. FINANCIAL INSTITUTION SHALL BE RESPONSIBLE ONLY FOR PERFORMING THE SERVICES EXPRESSLY PROVIDED FOR IN THIS AGREEMENT, AND SHALL BE LIABLE ONLY FOR ITS GROSS NEGLIGENCE OR WILLFUL MISCONDUCT IN PERFORMING THOSE SERVICES. FINANCIAL INSTITUTION SHALL NOT BE RESPONSIBLE FOR MEMBER'S ACTS OR OMISSIONS (INCLUDING, WITHOUT LIMITATION, THE AMOUNT, ACCURACY, TIMELINESS OF TRANSMITTAL OR AUTHORIZATION OF ANY ENTRY RECEIVED FROM MEMBER) OR THOSE OF ANY OTHER PERSON, INCLUDING, WITHOUT LIMITATION, ANY FEDERAL RESERVE BANK, ACH OPERATOR OR TRANSMISSION OR COMMUNICATIONS FACILITY, ANY RECEIVER OR RDFI (INCLUDING, WITHOUT LIMITATION, THE RETURN OF ANY ENTRY BY SUCH RECEIVER OR RDFI), AND NO SUCH PERSON SHALL BE DEEMED FINANCIAL INSTITUTION'S AGENT. MEMBER AGREES TO INDEMNIFY FINANCIAL INSTITUTION AGAINST ANY LOSS, LIABILITY OR EXPENSE (INCLUDING ATTORNEYS' FEES AND COSTS) RESULTING FROM OR ARISING OUT OF ANY CLAIM OF ANY PERSON THAT THE FINANCIAL INSTITUTION IS RESPONSIBLE FOR ANY ACT OR OMISSION OF MEMBER OR ANY OTHER PERSON DESCRIBED IN THIS SECTION 29(a).
- b) FINANCIAL INSTITUTION SHALL BE LIABLE FOR MEMBER'S ACTUAL DAMAGES DUE TO CLAIMS ARISING SOLELY FROM FINANCIAL INSTITUTION'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT; IN NO EVENT SHALL FINANCIAL INSTITUTION BE LIABLE FOR ANY CONSEQUENTIAL, SPECIAL, INCIDENTAL, PUNITIVE OR INDIRECT LOSS OR DAMAGE WHICH MEMBER MAY INCUR OR SUFFER IN CONNECTION WITH THIS AGREEMENT, WHETHER OR NOT THE LIKELIHOOD OF SUCH DAMAGES WAS KNOWN OR CONTEMPLATED BY THE FINANCIAL INSTITUTION AND REGARDLESS OF THE LEGAL OR EQUITABLE THEORY OF LIABILITY WHICH MEMBER MAY ASSERT, INCLUDING, WITHOUT LIMITATION, LOSS OR DAMAGE FROM SUBSEQUENT WRONGFUL DISHONOR RESULTING FROM FINANCIAL INSTITUTION'S ACTS OR OMISSIONS PURSUANT TO THIS AGREEMENT.

- c) WITHOUT LIMITING THE GENERALITY OF THE FOREGOING PROVISIONS, FINANCIAL INSTITUTION SHALL BE EXCUSED FROM FAILING TO ACT OR DELAY IN ACTING IF SUCH FAILURE OR DELAY IS CAUSED BY LEGAL CONSTRAINT, INTERRUPTION OF TRANSMISSION OR COMMUNICATION FACILITIES, EQUIPMENT FAILURE, WAR, EMERGENCY CONDITIONS OR OTHER CIRCUMSTANCES BEYOND FINANCIAL INSTITUTION'S CONTROL. IN ADDITION, FINANCIAL INSTITUTION SHALL BE EXCUSED FROM FAILING TO TRANSMIT OR DELAY IN TRANSMITTING AN ENTRY IF SUCH TRANSMITTAL WOULD RESULT IN FINANCIAL INSTITUTION'S HAVING EXCEEDED ANY LIMITATION UPON ITS INTRA- DAY NET FUNDS POSITION ESTABLISHED PURSUANT TO PRESENT OR FUTURE FEDERAL RESERVE GUIDELINES OR IN FINANCIAL INSTITUTION'S REASONABLE JUDGMENT OTHERWISE WOULD VIOLATE ANY PROVISION OF ANY PRESENT OR FUTURE RISK CONTROL PROGRAM OF THE FEDERAL RESERVE OR ANY RULE OR REGULATION OF ANY OTHER U.S. GOVERNMENTAL REGULATORY AUTHORITY.
- d) SUBJECT TO THE FOREGOING LIMITATIONS, FINANCIAL INSTITUTION'S LIABILITY FOR LOSS OF INTEREST RESULTING FROM ITS ERROR OR DELAY SHALL BE CALCULATED BY USING A RATE EQUAL TO THE AVERAGE FEDERAL FUNDS RATE AT THE FEDERAL RESERVE BANK OF NEW YORK FOR THE PERIOD INVOLVED. AT FINANCIAL INSTITUTION'S OPTION, PAYMENT OF SUCH INTEREST MAY BE MADE BY CREDITING THE ACCOUNT.

30. **INCONSISTENCY OF NAME AND ACCOUNT NUMBER.** The Member acknowledges and agrees that, if an Entry describes the Receiver inconsistently by name and account number, payment of the Entry transmitted by the Financial Institution to the RDFI may be made by the RDFI (or by the Financial Institution in the case of an On-US Entry) on the basis of the account number supplied by the Member, even if it identifies a person different from the named Receiver, and that the Member's obligation to pay the amount of the Entry to the Financial Institution is not excused in such circumstances. Member is liable for and must settle with Financial Institution for any Entry initiated by Member that identifies the Receiver by account or identifying number or by name and account or identifying number.

31. **PAYMENT FOR SERVICES.** The Member shall pay the Financial Institution the charges for the services provided in connection with this Product Schedule, as set forth in the deposit fee schedules and pricing proforma provided at time of application. All fees and services are subject to change upon thirty (30) days prior written notice from the Financial Institution. Such charges do not include, and the Member shall be responsible for payment of, any sales, use, excise, value added, utility or other similar taxes relating to such services, and any fees or charges provided for in the Depository Agreement between the Financial Institution and the Member with respect to the Account.

32. **AMENDMENTS.** Except as provided in Section 31, the Financial Institution may amend this Product Schedule from time to time upon written notice to the Member. In the event that performance of services under this Product Schedule would result in a violation of any present or future statute, regulation or governmental policy to which the Financial Institution is subject, then this Product Schedule shall be amended to the extent necessary to comply with such statute, regulation or policy. Alternatively, the Financial Institution may terminate this Product Schedule if it deems such action necessary or appropriate under the circumstances. The Financial Institution shall have no liability to the Member as a result of any such violation, amendment or termination. Any practices or course of dealings between the Financial Institution and the Member, or any procedures or operational alterations used by them, shall not constitute a modification of this Product Schedule or the Rules, nor shall they be construed as an amendment to this Product Schedule or the Rules.

**33. NOTICES, INSTRUCTIONS, ETC.**

- a) Except as stated herein, the Financial Institution shall not be required to act upon any notice or instruction received from the Member or any other person, or to provide any notice or advice to the Member or any other person with respect to any matter.
- b) The Financial Institution shall be entitled to rely on any written notice or other written communication believed by it in good faith to be genuine and to have been signed by an authorized representative of Member, and any such communication shall be deemed to have been signed by such person. Such notice shall be effective on the second Business Day following the day received by the Financial Institution.
- c) Except as stated herein, any written notice or other written communication required or permitted to be given under this Product Schedule shall be delivered or sent by US mail, if to Member, at the address of Member on the books of Financial Institution and if to Financial Institution, at the following address:

Center Parc Credit Union  
Attn: ACH Department  
400 Porsche Avenue  
Atlanta, GA 30354

unless another address is substituted by notice delivered or sent as provided heron. Except as otherwise stated herein, any such notice shall be deemed given when received.

34. **DATA RETENTION AND PROTECTION.** The Member shall retain data on file adequate to permit the remaking of Entries for five (5) Business Days following the date of their transmittal by the Financial Institution as provided herein, and shall provide such Data to the Financial Institution upon its request. Member acknowledges and agrees to comply with any and all Data Security Requirements contained in the Rules, including without limitation any requirements of ACH Originators, Third-Party Service Providers and Third-Party Senders to protect account numbers used in the initiation of ACH Entries and Files by rendering them unreadable when stored electronically.
35. **DATA MEDIA AND RECORDS.** All magnetic tapes, Entries, security procedures and related records used by the Financial Institution for transactions contemplated by this Product Schedule shall be and remain the Financial Institution's property. The Financial Institution may, at its sole discretion, make available such information upon the Member's request. Any expenses incurred by the Financial Institution in making such information available to the Member shall be paid by the Member.
36. **COOPERATION IN LOSS RECOVERY EFFORTS.** In the event of any damages for which Financial Institution or Member may be liable to each other or to a third party pursuant to the services provided under this Product Schedule, Financial Institution and Member will undertake reasonable efforts to cooperate with each other, as permitted by applicable law, in performing loss recovery efforts and in connection with any actions that the relevant party may be obligated to defend or elects to pursue against a third party.
37. **TERMINATION.** In addition to, and without limiting the generality of, the Termination provisions of the Master Agreement, Financial Institution may terminate this Product Schedule immediately upon its determination that Member is in violation of this Product Schedule, the ACH Rules or applicable laws or if Member initiates any bankruptcy proceeding or is otherwise declared insolvent. Any termination of this Product Schedule shall not affect any of Financial Institution's rights or Member's obligations with respect to any Entries initiated by Member prior to such termination, or the payment obligations of Member with respect to services performed by Financial Institution prior to termination, or any other obligations that survive termination of this Product Schedule. Member's obligation with respect to any Entry shall survive termination of this Product Schedule until any applicable statute of limitation has elapsed.
38. **ENTIRE AGREEMENT.** This Product Schedule (including the Schedules attached) together with the Depository Agreement and the Master Agreement, is the complete and exclusive statement of the agreement between the Financial Institution and the Member with respect to the subject matter hereof and supersedes any prior agreement(s) between the Financial Institution with respect to such subject matter. In the event of any inconsistency between the terms of this Product Schedule, the Depository Agreement or the Master Agreement, the terms of this Product Schedule shall govern. In the event performance of the services provided herein in accordance with the terms of this Product Schedule would result in a violation of any present or future statute, regulation or government policy to which the Financial Institution is subject, and which governs or affects the transactions contemplated by this Product Schedule, then this Product Schedule shall be deemed amended to the extent necessary to comply with such statute, regulation or policy, and the Financial Institution shall incur no liability to the Member as a result of such violation or amendment. No course of dealing between the Financial Institution and the Member will constitute a modification of this Product Schedule, the Rules, or the security procedures, or constitute an agreement between the Financial Institution and the Member regardless of whatever practices and procedures the Financial Institution and the Member may use.
39. **NON-ASSIGNMENT.** The Member may not assign this Agreement or any of the rights or duties hereunder to any person without the Financial Institution's prior written consent.
40. **WAIVER.** The Financial Institution may waive enforcement of any provision of this Agreement. Any such waiver shall not affect the Financial Institution's rights with respect to any other transaction or modify the terms of this Agreement.
41. **BINDING AGREEMENT; BENEFIT.** This Agreement shall be binding upon and inure to the benefit of the parties

hereto and their respective legal representatives, successors, and assigns. This Agreement is not for the benefit of any other person, and no other person shall have any right against the Financial Institution or the Member hereunder.

- 42. **HEADINGS.** Headings are used for reference purposes only and shall not be deemed part of this Agreement.
- 43. **SEVERABILITY.** In the event that any provision of this Agreement shall be determined to be invalid, illegal, or unenforceable to any extent, the remainder of this Agreement shall not be impaired or otherwise affected and shall continue to be valid and enforceable to the fullest extent permitted by law.
- 44. **GOVERNING LAW.** This Agreement shall be construed in accordance with and governed by the laws of the State of Georgia without reference to its conflict of laws, provisions, and applicable federal law.
- 45. **SAME DAY ENTRIES.** If Same Day ACH is offered by Financial Institution, a credit or debit Entry with an Effective Entry Date of the date of or a date prior to the date of the transmission of the Entry or File to Credit Union and received by Credit Union prior to the applicable cut-off time set forth in Schedule B shall be considered a Same Day Entry. Entries in excess of the amount permitted in the Rules and IAT Entries are not eligible for Same Day ACH processing. In addition to any other fees that Member is obligated to pay Credit Union, Member hereby agrees to pay Credit Union the Same Day Entry fee established by Credit Union from time to time for Same Day Entries transmitted to Credit Union by Member.
- 46. **PRINCIPAL/OWNER GUARANTY.** The undersigned hereby guarantees the prompt payment and performance of all amounts, fees, and obligations of the member due and owing to Center Parc (Financial Institution) arising under or in connection with that certain Member Agreement for ACH Origination (the "Agreement"), dated of even date herewith between Member and Financial Institution. This Guaranty is intended to cover all obligations of Member under the Agreement, including, but not limited to, (a) the payment of fees and amounts arising under the Agreement or in connection with any deposit account maintained by Member with Financial Institution, (b) the compliance by Financial Institution with all laws, regulations and rules related to Member's origination and processing of ACH Entries under the Agreement, (c) Member's obligations with respect to Reserves and the return of ACH Entries under the Agreement and (d) the accuracy and performance of Member's warranties under the Agreement. In order to secure the payment and performance of this Guaranty, the undersigned hereby grants to Financial Institution a security interest in and to all deposit accounts owned by the undersigned and maintained at Financial Institution. The undersigned hereby agrees and acknowledges that this Guaranty is a guarantee of performance and not of collection, and that Financial Institution may, upon default or violation by Member of any terms of the Agreement, proceed directly against the undersigned for satisfaction and performance of the obligations of Member under the Agreement without first proceeding against Member.

**This Product Schedule must be signed on behalf of Member by an Authorized Member Representative.**

**IN WITNESS WHEREOF,** the parties hereto have executed this Product Schedule through their duly authorized officers on the dates indicated below.

\_\_\_\_\_  
Dated:

\_\_\_\_\_  
Company's Legal Name

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Print Name

## Schedule A

# Center Parc Credit Union ACH Origination Services Training Guide March 2026

Center Parc Credit Union is pleased to provide ACH Origination Services. While we recommend that you read and become familiar with the Nacha Operating Rules, this guide was developed to give you an overview of important information you should be aware of as an ACH Originating member. This guide is to assist you with training, compliance, and risks associated with ACH Origination.

## WHAT IS THE ACH NETWORK?

The Automated Clearing House (ACH) Network is a nationwide electronic payment system that enables individuals, businesses, financial institutions, and government agencies to electronically send and receive funds. It supports both credit and debit transactions, allowing money to be moved between checking accounts, savings accounts, general ledger accounts, and even loan accounts.

Serving as a central infrastructure for electronic payments, the ACH Network provides a secure, reliable, and efficient method for processing a wide range of transactions. It connects virtually all U.S. banks and credit unions and handles billions of payments each year, including Direct Deposit and Direct Payment transactions. The network operates in a batch-processing environment and is jointly governed and utilized by financial institutions of all sizes.

## WHO IS NACHA?

The National Automated Clearing House Association (“Nacha”) Nacha is a not-for-profit association representing financial institutions directly and through regional payments associations. It develops the operating rules and business practices that govern the ACH Network and supports standards for a wide range of electronic payments, including online commerce, electronic bill payment, electronic check conversion, financial data exchange, international payments, and electronic benefit services.

## REVISIONS TO THE NACHA OPERATING RULES (ANNUAL)

Annually, you will receive a letter from the Credit Union explaining changes in the Nacha rules. These changes are described in the Revisions to the Nacha Operating Rules section of the rule book. The changes will cover the time period of January 1 to December 31 of that year. If you have questions about the revisions, please contact us.

## DEFINITION OF ACH PARTICIPANTS

- **Originator** – The Originator is the entity or company that agrees to initiate ACH entries into the payment system according to an arrangement with a Receiver. The Originator is usually a company directing a transfer of funds to or from a consumer or another company’s account.

- **Originating Depository Financial Institution (ODFI)** – The ODFI is the financial institution that receives the payment instructions from Originators and forwards the entries to the ACH Operator.
- **Automated Clearing House Operator** – An ACH Operator is the central clearing facility operated by a private organization or the Federal Reserve Bank (FRB) on behalf of Depository Financial Institutions.
- **Receiving Depository Financial Institution (RDFI)** – The RDFI is the Depository Financial Institution that receives ACH entries from the ACH Operator and posts the entries to the accounts of its depositors (Receivers).
- **Receiver** – A Receiver is a natural person or an organization that has authorized an Originator to initiate an ACH entry to the Receiver’s account with the RDFI. A Receiver may be either a company or a consumer, depending on the type of transaction.

## **ACH LEGAL FRAMEWORK**

You are required to abide by multiple rules and agreements including, but not limited to, the following when submitting ACH transactions. The Credit Union may ask for access to your premises and records to confirm compliance with ACH Rules.

The Credit Union has the right to audit your compliance with the Nacha Operating Rules and your compliance with the Origination Agreement at any time. The Credit Union has the right to terminate the Origination Agreement immediately for breach of the Nacha Operating Rules or applicable laws.

- Nacha Operating Rules
- BSA/AML
- OFAC
- 31 CFR Part 210
- Regulation E (for consumer entries)
- UCC4A (for corporate credits)
- Credit Union Deposit Agreement & Terms and Conditions
- Credit Union Business Online Banking & Cash Management Agreement
- Credit Union ACH Origination Product Schedule
- Authorizations from employees, customers, etc.

## **HOW THE ACH NETWORK FUNCTIONS**

The ACH process begins when an Originator obtains proper authorization—or provides required notice—to a Receiver to initiate an electronic debit or credit. The Originator compiles these authorized transactions into an ACH file and submits it to its Originating Depository Financial Institution (ODFI). The ODFI collects ACH files from all its Originators, validates formatting and content, and then transmits them in scheduled batches to an ACH Operator, sometimes excluding “on-us” entries involving its own account holders.

The ACH Operator—either the Federal Reserve or a private-sector operator—receives and edits these files for compliance and accuracy before routing the appropriate entries to each Receiving Depository Financial Institution (RDFI). The RDFI then posts the incoming entries to customer accounts according to the Settlement Date and account information, and Receivers later see these transactions reflected on their periodic account statements.

Because the ACH Network functions as a same-day, batch, store-and-forward system, transactions are collected and processed at designated intervals rather than in real time. This framework enables the secure, standardized exchange of funds and payment information across the United States, its territories, and internationally, supporting broad adoption of efficient electronic payments.

## HOW ACH FUNDS ARE SETTLED

ACH settlement is the process by which funds actually move between financial institutions to complete an ACH payment. Settlement occurs only on banking days, and the Federal Reserve Bank (FRB) provides settlement services for all ACH transactions—whether they are processed through the Federal Reserve’s ACH Operator or a private-sector operator like EPN. During this process, the Federal Reserve calculates each institution’s net debit or credit and posts the amount to that institution’s reserve account or the account of its correspondent bank.

Settlement timing depends on two key factors:

1. **Effective Entry Date:** The date specified by the Originator to indicate when the entry should post to the Receiver’s account.
2. **Delivery time of the ACH file to the ACH Operator:** When the Operator receives the file, it uses the Effective Entry Date to assign the corresponding Settlement Date.

Entries settle on the assigned Settlement Date. If the Effective Entry Date falls on a weekend or holiday, or if the file arrives too late for timely processing, settlement automatically shifts to the next business day. Although the Effective Entry Date and Settlement Date typically match, late file delivery, stale dates, or non-banking days can delay settlement.

Historically, the ACH Network has used a settlement cycle of one to two business days after processing. Debit entries may be sent to the ACH Operator one day before their Effective Entry Date, while credit entries may be sent up to two days in advance. This standard timeline is still in place; however, Originators may also choose Same Day ACH, which allows eligible debits and credits to be processed and settled within the same business day.

## ACH RULES AND REGULATIONS

ACH transactions are governed by multiple rules and regulatory frameworks that outline responsibilities for financial institutions and protect consumers. The Nacha Operating Rules serve as the primary framework for ACH payments, defining participant obligations, establishing processing standards, and supporting risk-reduction across the Network.

In addition to Nacha Rules, financial institutions must comply with several federal requirements:

- **OFAC** regulations require monitoring for sanctioned individuals and entities as part of U.S. economic sanctions programs.
- **Regulation E** implements the Electronic Fund Transfer Act, establishing consumer rights and institutional responsibilities for electronic payments. (Supported broadly under ACH consumer protections referenced in ACH processing descriptions.)
- **31 CFR Part 210** governs the use of the ACH Network for federal government payments and outlines responsibilities for federal agencies and financial institutions.

- **UCC Article 4A** governs commercial ACH credit transactions and outlines obligations for corporate payment handling. (Supported indirectly through ODFI/RDFI commercial transaction descriptions.)
- **BSA/AML** requirements obligate institutions to monitor ACH activity for unusual or suspicious behavior as part of broader anti-money-laundering controls. (Supported through general ACH risk-monitoring expectations referenced in Nacha's fraud-monitoring rules.)

Financial institutions must ensure compliance with all applicable federal and state laws. When rules conflict, the most protective or restrictive requirement—typically the one benefiting the consumer—applies.

## ACH Transactions

The ACH Network provides an efficient way for consumers and businesses to make electronic payments, supporting functions such as direct deposit of payroll, automated bill payments, online purchases, cash concentration, and corporate-to-corporate transfers. As the shift from paper to digital payments continues, the ACH Network's cost-effective electronic framework plays an increasingly important role in enabling reliable, streamlined payment activity.

### TYPES OF ACH TRANSACTIONS

ACH transactions are generally divided into two main categories:

- **Commercial Entries**  
These are payments initiated by private-sector organizations, including state and local government entities. They are frequently used for payroll deposits, bill payments, and a wide range of business-to-business transactions.
- **Government Entries**  
These entries are originated by federal agencies and are commonly used for payments such as Social Security benefits and other federal disbursements.

### COMMON USES OF COMMERCIAL ACH TRANSACTIONS

- **Direct Deposit (ACH Credits)**  
Direct Deposit uses ACH credit entries to place funds directly into a consumer's account. This method is used for payroll, tax refunds, reimbursements, government benefits, and similar payments. It provides faster availability of funds compared to paper checks.
- **Direct Payment (ACH Credits or Debits)**  
Direct Payment allows individuals or organizations to make either recurring or one-time payments. These can include online-initiated payments and transactions created through check conversion. Businesses increasingly rely on Direct Payment for B2B transactions because it reduces the cost of processing checks, improves cash-flow timing, and supports addenda records that transmit detailed payment information.

## AUTHORIZATIONS

You must obtain the Receiver’s authorization which must be signed or similarly authenticated by the consumer.

- You must provide a copy of the authorization to the Receiver.

The Authorization must:

- 1) Be readily identifiable as an ACH authorization.
  - 2) Have clear and readily understandable terms.
  - 3) Provide that the Receiver may revoke the authorization only by notifying you in the time and manner specified in the authorization.
- The authorization must be kept for two years following the termination or revocation of the authorization.
  - If a copy of an authorization is requested by the Credit Union, you must supply it so that we can respond to the RDFI’s request. We have 10 Banking Days to provide the RDFI with the Authorization.
  - If the Entry is a recurring debit you are required to notify the Receiver of any changes in the date or dollar amount.
    - At least seven (7) calendar days prior to a change in the date (consumer and corporate).
    - At least ten (10) calendar days prior to the change in the dollar amount (consumer only), unless it is within the agreed upon amount. Refer to the *Nacha Operating Rules and Guidelines*, for clarification, or contact us at the number listed).
  - Cease subsequent entries when notified.
  - The Receiver’s (your customer/employee) Financial Institutions deposit tickets should not be used to obtain the Financial Institution’s routing number. These most often have internal processing numbers.

An authorization may restrict an Originator to debit-only or credit-only entries and may specify either a fixed amount or a variable amount. ACH authorizations should also include language acknowledging that ACH entries must comply with applicable U.S. laws.

SEC CODES	ENTRY TYPE	AUTHORIZATION PROTOCOLS
Accounts Receivable Entry (ARC) (Corporate to Consumer/Corporate to Corporate)	Debits	Notice is required prior to accepting the check to authorize its conversion to an ACH debit.
Back Office Conversion (BOC) (Corporate to Consumer/Corporate to Corporate)	Debits	Notice is required prior to accepting the check to authorize its conversion to an ACH debit.
Corporate Credit or Debit (CCD) (Corporate to Corporate)	Debits/ Credits	An agreement is required for transfers between companies, and written authorization is implied.
Customer-Initiated Entry (CIE) (Consumer to Corporate)	Credits	A presumed agreement exists between the consumer and the company or paying agent.
Corporate Trade Exchange (CTX) (Corporate to Corporate)	Debits/ Credits	An agreement is required for transfers between companies, and written authorization is implied.

International ACH Transaction (IAT) (Corporate to Corporate/Corporate to Consumer/ Consumer to Consumer)	Debits/ Credits	Transfers between companies require an agreement. Credit entries to consumer accounts may be authorized orally or by other non-written means, while debit entries to consumer accounts require a written, signed, or similarly authenticated authorization.
Point-of-Purchase Entry (POP) (Corporate to Consumer/Corporate to Corporate)	Debits	Notice must be provided before accepting the check, and a written, signed, or similarly authenticated authorization is required.
Prearranged Payment & Deposit (PPD) (Corporate to Consumer)	Credits	Authorization is required, and oral or other non-written methods (such as a voided check) are acceptable.
Prearranged Payment & Deposit (PPD) (Corporate to Consumer)	Debits	Authorization is required and must be written, signed, or similarly authenticated. For Return Fee Entries, authorization may be obtained by providing notice to the consumer when the original debit is presented.
Re-presented Check Entry (RCK) (Corporate to Consumer)	Debits	Notice is required prior to accepting the check to authorize its conversion to an ACH debit.
Telephone-Initiated Entry (TEL) (Corporate to Consumer)	Debits	For Single Entry, the authorization must be a recorded oral authorization or a written confirmation provided to the consumer. For Recurring payments, a copy of the authorization must be given to the consumer, or a standing authorization must already be in place.
Internet-Initiated/Mobile Entry (WEB) (Corporate to Consumer)	Debits	A similarly authenticated authorization is required due to the online nature of the transaction.
Internet-Initiated/Mobile Entry (WEB) (Consumer to Consumer)	Credits	No authorization is required.
Destroyed Check Entry (XCK)	Debits	No authorization is required.
Point-of-Sale (POS)	Debits/Credits	Written, signed, or similarly authenticated authorization is required.

## PRE-NOTIFICATIONS

Pre-notifications are non-dollar Entries used to verify that the account number and routing number is valid.

- Pre-notes are optional for you to send. However, if sent, pre-note rules must be followed and a pre-note must precede the first live entry by at least three (3) Banking Days prior to the first live dollar Entry.
- Make sure the name you use for your company is easily recognizable to the customer. If you must abbreviate your name, make sure it is understandable to the customer. This is what they will see on their bank statement.
- Do not use Center Parc's name.
- The Receiving Bank is not required to validate the name of the payee on the pre-note, although many do; they are only required to check the account number.
- If the pre-note does not contain a valid account number, or is otherwise processable, you will receive either:
  - A return Entry, or
  - NOC
- You must correct the inaccurate information before submitting the next live entry.

## ORIGINATION FILE

\*In this example we used the Standard Entry Class (SEC) codes PPD & CCD, others can be found in the *Nacha Operating Rules and Guidelines*.

- Have you used the correct SEC Code for the File you are sending?
  - A Payroll File is a credit going to a Consumer account and should have the SEC Code of PPD.
  - A fee or payment is a debit from a consumer account and should have the SEC code of PPD.
  - Collection of Utility Payments from a Business/Corporation the SEC used should be CCD.
  - Credit or Debit from a Corporate to a Corporate the SEC Code should be CCD.
  - If you are collecting payments for both Consumer and Corporate, they should be originated as two separate batches.
  - The CCD SEC code has a 2-Banking Day return time frame and the PPD SEC code has a 60 calendar-day return time frame.
  - The Company Name Field should be populated with a name that is readily recognized as the Receiver of the Entry.
  - The Company Entry Description Field should provide the Receiver with a description of the purpose of the Entry, (i.e. Payroll, Condo Fee, Utility Payment).
- Send entries on the proper date.

## COMPANY ENTRY DESCRIPTION

- For PPD Credits related to wages, salaries, and other similar types of compensation, the ACH Originator must use the term "PAYROLL" in the company entry description field.

## NOTICE OF CHANGE (NOC)

- A NOC is a non-dollar Entry transmitted by an RDFI to notify you that information obtained within an Entry is erroneous and/or has become outdated and must be changed.
- The ACH Rules require you, the company, to make the requested change within six (6) Banking Days of receipt of the NOC or prior to the initiation of another ACH Entry.
- Failure by you to respond to NOCs may result in fines to the Credit Union.
- Call the Credit Union at (800) 849-8431 if you have any questions.

## RETURNED ENTRIES

- An ACH return is an ACH Entry that the RDFI is unable to post for reasons defined by the return codes.
- The following return reason codes must be returned within 2 Banking Days of receiving it. If you receive a return Entry, with one of the following return reasons, except for R01, you must stop initiating the Entries and contact the Receiver:
  - R01 – Insufficient Funds (see Reinitiation of Return Entries)
  - R02 – Account Closed

- R03 – No Account
- R04 – Invalid Account
- R08 – Payment Stopped (A stop payment may be for one, several or all future Entries. You may not reinitiate the returned Entry unless the reason for the return is remedied. Contact the customer to determine the intent of the return.)
- R29 – Corporate Customer Advises not Authorized
- The following return reason codes can be returned up to 60 calendar days later if they are associated with a consumer SEC code. If you receive a return with one of these return reasons you must stop initiating the Entries. If a valid authorization exists, you may have recourse outside the ACH Network. Keep in mind you could receive these back as late as 60 calendar days after you first initiated them. A Consumer must complete a Written Statement of Unauthorized Debit (WSUD) form when requesting an Entry be returned for one of these reasons. You may request a copy of the WSUD from your Financial Institution.
  - R05 – Unauthorized Debit to a Consumer Account using Corporate SEC code
  - R07 – Authorization Revoked
  - R10 – Customer Advises Originator is Not Known to Receiver and/or Originator is Not Authorized by Receiver to Debit Receivers Account
  - R11 – Customer Advised Entry Not in Accordance with the Terms of the Authorization
  - R37 – Source Document Presented for Payment
  - R51 – Item Related to RCK Entry is Ineligible or RCK Entry is Improper.

## **REINITIATION OF RETURN ENTRIES**

- You may reinitiate an Entry that has been previously returned (other than an RCK) if:
  - The Entry was returned for insufficient or uncollected funds.
  - The Entry was returned as stop payment and reinitiation has been authorized by the Receiver.
  - Corrective Action was taken to remedy the reason for the return (Example R11).
- Entry must be reinitiated within 180 days of settlement of the original Entry.
- You must not reinitiate an Entry that has been returned for insufficient or uncollected funds more than two times following the return of the original Entry (for a total of three times).
- The Entry was returned as stop payment and reinitiation has been separately authorized by the Receiver.
- Originator must submit Reinitiated Entries as a separate batch that contains the word ‘RETRY PYMT’ in the Company Entry Description field of the Company/Batch Header Record.

## **REVERSALS**

- As an Originator you may reverse an erroneous or duplicate ACH Entry/File up to 5 Banking Days after the Settlement Date of the Entry/File.
  - Erroneous Entry – an Entry that (a) is a duplicate of an Entry previously initiated by the Originator or ODFI; (b) orders payment to or from a Receiver different than the Receiver intended to be credited or debited by the Originator; or (c) orders payment in a dollar amount different than was intended by the Originator.

- A reversal is **not a guarantee** the File will be reversed. If there are not sufficient funds in the Receiver's account when the reversal is received by the receiving Financial Institution the reversal can be returned back to you.

## OFAC (OFFICE OF FOREIGN ASSET CONTROL)

- You are required to check payees against OFAC compliance checklists.
- OFAC list countries, groups and individuals with which U.S. Companies are not permitted to send or receive funds.
- The Credit Union must protect itself by informing every ACH Originator that it is against the law to send debit or credit entries to OFAC-blocked entities.
- You may check the OFAC Sanctions list at: [Sanctions List Search Tool | Office of Foreign Assets Control](#)

## INTERNATIONAL ACH TRANSACTIONS

The ACH Network can also facilitate cross-border payments. In these cases, a Gateway participant handles tasks such as currency conversion, settlement, and mapping foreign payment formats into ACH-compatible structures.

## TRANSACTION CODES

The ACH Network supports several different credit and debit applications. A Transaction Code identifies an entry as a debit or credit and indicates the type of account to which the transaction is intended, i.e. checking, savings, or financial institution general ledger. Commonly used Transactions Codes are listed below:

### **Demand (Checking) Credits**

- 21 Notification of Change or Return
- 22 Demand Credit (Deposit)
- 23 Prenotification for a Demand Credit (Deposit)
- 24 Zero Dollar Entries w/Remittance Data (for CCD and CTX Entries Only)

### **Demand (Checking) Debits**

- 26 Notification of Change or Return
- 27 Demand Debit (Payment)
- 28 Prenotification for Demand Debit (Payment)
- 29 Zero Dollar Entries w/Remittance Data (for CCD and CTX Entries Only)

### **Savings Account Credits**

- 30 Notification of Change or Return
- 31 Savings Credit (Deposit)
- 32 Prenotification for Savings Credit (Deposit)
- 33 Zero Dollar Entries w/Remittance Data (for CCD and CTX Entries Only)

### Savings Account Debits

- 36 Notification of Change or Return
- 37 Savings Debit (Payment)
- 38 Prenotification for Savings Debit (Payment)
- 39 Zero Dollar Entries w/Remittance Data (for CCD and CTX Entries Only)

### Financial Institution General Ledger (GL) Credits

- 41 Notification of Change or Return
- 42 GL Credit
- 43 Prenotification for GL Credit
- 44 Zero Dollar Entries w/Remittance Data (for CCD and CTX Entries Only)

### Financial Institution General Ledger (GL) Debits

- 46 Notification of Change or Return
- 47 GL Debit
- 48 Prenotification of GL Debit
- 49 Zero Dollar Entries w/Remittance Data (for CCD and CTX Entries Only)

## STANDARD ENTRY CLASS (SEC) Codes

A Standard Entry Class (SEC) Code is a three-character identifier that defines the type of ACH entry being transmitted, and each code carries its own specific set of requirements.

An SEC Code outlines important characteristics of an ACH transaction, including:

- Whether the entry is consumer or corporate/business, and whether it represents a single transaction or a recurring series.
- The ACH Rules and regulatory requirements that apply, such as the proper method for obtaining authorization or providing required notices.
- The precise record format used to transmit the payment and any accompanying information.

Understanding the SEC Code for an ACH entry is essential because it determines how the entry must be posted and how any returns must be handled. For financial institutions, accurate interpretation of SEC Codes is critical to minimizing errors and preventing operational losses. Below are the most frequently used SEC Codes and their primary purposes.

SEC CODE	SEC CODE DESCRIPTION	PRACTICAL APPLICATION
ARC	Accounts Receivable Entry	The Accounts Receivable (ARC) Entry allows billers to convert customer checks into single-entry ACH debits when checks are received by mail, at a drop box, or in person. Customers must be notified beforehand that submitting a check serves as authorization for an ARC debit. The check is then used only to obtain the routing number, account number, and check serial number needed to process the ACH entry.
BOC	Back Office Conversion	Back Office Conversion (BOC) lets retailers and billers convert checks received at checkout or at a staffed payment location into single-entry ACH debits. Customers authorize this conversion through posted notice and by presenting their check. The conversion decision is made later in the back office, and the check issued only to obtain the routing number, account number, and check serial number needed for the ACH debit.

<b>CCD</b>	Corporate Credit or Debit	The Corporate Credit or Debit (CCD) application enables companies to move funds quickly, manage cash flow, and streamline disbursements. It allows businesses with multiple locations to consolidate funds efficiently and improve cash-management predictability. CCD entries can also be used for payments between corporate entities and can include limited remittance information such as invoice numbers or purchase order details.
<b>CIE</b>	Customer-Initiated Entry	A credit entry initiated by consumers through a bill payment service provider to pay bills, including bill payment services submitted through a telephone, ATM or online.
<b>CTX</b>	Corporate Trade Exchange	The Corporate Trade Exchange (CTX) application enables companies to electronically send and receive payments along with detailed remittance information. It is commonly used for business-to-business payments, replacing paper checks with ACH debits and credits processed between the companies' financial institutions.
<b>IAT</b>	International ACH Transaction	An International ACH Transaction (IAT) is a credit or debit ACH entry tied to a payment involving a financial agency located outside the United States. IAT entries can be sent to or from consumer or corporate accounts and must include seven mandatory addenda records, which provide the Originator's and Receiver's names and physical addresses, the Receiver's account and bank information, and the purpose of the payment.
<b>POP</b>	Point-of-Purchase Entry	The Point-of-Purchase (POP) application lets businesses convert a customer's in-person check into a one-time ACH debit at the point of sale or a staffed payment location. After proper notice, the merchant captures the routing number, account number, and check serial number using a check reader and manually enters the transaction amount. The check is then voided and returned to the customer, who authorizes its conversion into an electronic debit.
<b>POS</b>	Point-of-Sale	Point-of-Sale (POS) entries are ACH debits initiated when a customer uses a merchant-issued card to make a purchase. The card is swiped and validated as active and within limits, but the customer's account balance is not checked, nor is the account immediately debited. Instead, the transaction settles later when the card issuer creates a POS ACH entry to withdraw the funds from the customer's account.
<b>PPD</b>	Prearranged Payment and Deposit	Prearranged Payments and Deposits (PPD) allow single or recurring ACH credits or debits, commonly known as Direct Deposit and Direct Payment. Direct Deposit sends funds to consumer accounts, while Direct Payment collects funds from them. PPD can also be used to assess return fees for NSF or UCF items when permitted by law and when proper notice is given.
<b>RCK</b>	Re-presented Check Entry	The Re-presented Check (RCK) entry allows businesses to collect funds on consumer checks that were returned for insufficient or uncollected funds. With proper notice, a returned check can be re-submitted as an ACH debit through the ACH Network to attempt collection again.
<b>TEL</b>	Telephone-Initiated Entry	The Telephone-Initiated Entry (TEL) allows businesses to debit a consumer's account based on an oral authorization given over the phone. TEL entries may be set up as a one-time payment or recurring payments. They may be used only when the Originator already has an existing relationship with the consumer, or when the consumer initiates the phone call to the Originator.
<b>WEB</b>	Internet-Initiated/Mobile Entry	The Internet-Initiated/Mobile (WEB) entry supports single or recurring ACH credits or debits authorized online or through a wireless network. WEB debits allow companies to collect payments for goods or services based on an online or mobile authorization. WEB credits allow consumers to send funds to another person or transfer money between their own accounts at different financial institutions. Payment instructions may be provided online, via mobile device, or in person at a financial institution.
<b>XCK</b>	Destroyed Check Entry	Destroyed Check Entries (XCK) are ACH debit entries used by an ODFI to collect funds on checks that were lost, destroyed, or otherwise unable to be processed through normal image exchange.

## DATA SECURITY

As an ACH Originator, your company plays a critical role in safeguarding Protected Information—the non-public personal (including financial) information of a natural person used to create, or contained within, an ACH Entry and any related Addenda Record.

Why this matters: Threats such as corporate account takeover, malware/viruses, network intrusions, employee/email fraud, and hacking are on the rise. Proper handling of Protected Information and ACH data helps prevent loss and operational disruptions.

Required security framework (per Nacha): Establish, implement, and regularly update policies, procedures, and systems related to the initiation, processing, and storage of ACH Entries and Protected Information to:

- Protect the confidentiality and integrity of Protected Information until secure destruction; no matter what form it is stored as, (e.g., electronically or paper based, from the point it is collected until it is destroyed).
- Guard against anticipated threats or hazards to that information; restrict and limit access to sensitive data.
- Use locks on doors and filing cabinets.
- Do not store sensitive information on portable devices as they are frequently lost or stolen.
- All portable data (e.g., CD's, USBs, reports and physical file folders) should be kept in secure areas.
- Prevent unauthorized use that could cause substantial harm to a natural person.

## **PROTECTING PERSONAL INFORMATION (FTC FIVE PRINCIPLES)**

To strengthen your overall data-security posture, follow the FTC's "Protecting Personal Information: A Guide for Business" framework:

1. Take Stock — Know what personal information you hold, where it resides, and who can access it (systems, devices, paper, third parties).
2. Scale Down — Collect and retain only what you need for business or legal reasons; implement retention schedules.
3. Lock It — Protect information you keep with physical, technical, and administrative safeguards (e.g., access controls, encryption in transit, vendor due diligence, employee training).
4. Pitch It — Dispose of data securely; do not discard sensitive records in regular trash.
5. Plan Ahead — Maintain an incident response plan for security events.

## **WHAT ARE THE FRAUD RISKS FOR ACH?**

ACH Origination fraud is a challenge for Financial Institutions and ACH Originators like your company. In one origination system hacking scheme, perpetrators hack into the Originator's (Your Company) computer system using compromised User IDs and passwords and originate ACH credits to "mule" accounts created for the express purpose of committing fraud. Those accounts are then emptied and abandoned. The true Originator's account (Your Account) is debited for the invalid origination file. The credits are usually irretrievable by the time fraud is discovered. The Originator's credentials may have been compromised by an insider within the organization or stolen through key loggers or Trojan Horse programs on the compromised computer.

Due to the risk of this type of fraud, it is essential that all computer equipment used by your company to operate the Credit Union's Cash Management ACH Origination program is regularly updated and patched for security vulnerabilities (including the use of and updating of firewall, virus protection, anti-malware

protection, anti-spam protection.) This ACH Origination Schedule requires using a dedicated computer that is not used for internet browsing or email and serves exclusively as your access point to the Cash Management system. Restricting activity on this device helps reduce the risk of downloading harmful software or viruses that could compromise ACH data and transactions

The appropriate steps should be taken within your company to ensure that all User ID's, Passwords, Authentication Methods and any other applicable security procedures issued to your employees are protected and kept confidential. All staff should be aware of the need for proper user security, password controls and separation of duties.

As ACH Origination is a higher risk commercial banking function, the Credit Union suggests that your company perform your own internal risk assessment and controls evaluation periodically to be sure you are considering all available security options.

For additional information on protecting your business online threats, please visit the Cybersecurity & Infrastructure Security Agency (CISA) website and view their "Secure Your Business" section for resources to protect your business, employees and customers with smart cybersecurity practices ([Secure Your Business | CISA](#)).

## **ORIGINATOR REQUIRED FRAUD MONITORING**

Each non-consumer Originator must establish and implement risk-based processes and procedures reasonably intended to identify ACH entries initiated due to fraud. All non-consumer ACH Originators will be required to do the following:

- **Establish risk-based processes and procedures** reasonably intended to identify Entries initiated due to fraud.
- **Identify Unauthorized or False Pretenses Entries** definition of false pretenses: Misrepresentation of 1) identity; 2) authority to act for another person; and 3) account ownership.
- **Annual Review Requirement** Originators must review the adequacy of their processes and procedures annually.
- **Monitoring must be meaningful and operational** monitoring must be documented and operational, not superficial or symbolic – *DOING NOTHING IS NOT ACCEPTABLE*.

***Refer to Appendix A for action items that support your compliance efforts.***

## **THE SAFEGUARDS IMPLEMENTED BY THE CREDIT UNION TO COMBAT ACH ORIGINATION FRAUD**

The business online banking platform provided by the Credit Union employs multi-factor authentication as a key security measure. Each user has an individual device/profile database, established through Internet data profiling that analyses IP addresses, ISP providers, geographic locations, and connection types used during login attempts. Once this profile is created, any attempt to log in from a previously unused PC or mobile device will trigger the Enhanced Login Security feature. This feature prompts users to select a masked phone number or email address on file to receive an access code, which must be entered before

access is granted.

Symantec™ VIP tokens further enhance security by supplying hacker-resistant multi-factor authentication for online banking transactions. These tokens generate a unique, one-time passcode every 30 seconds, ensuring that only successfully authenticated users can access online banking. Additionally, an email notification is sent immediately following the initiation of an ACH file, allowing users to promptly verify the transaction amount.

Despite these robust measures, risks such as internal fraud or external threats from sophisticated malware (e.g., keyloggers or Trojan horses) remain. To mitigate such risks, the Credit Union mandates separation of duties for ACH processing. One Credit Union employee initiates the ACH batch, while another—using Dual-Control procedures—must log in separately to approve it. This process significantly reduces the likelihood of ACH origination fraud.

It is also essential for companies to monitor their accounts online daily. By reviewing “Transaction History” screens within the Cash Management program each day, companies can stay informed about all account activity, even prior to transaction posting. Early detection of fraudulent activities increases the Credit Union’s ability to assist in recovering potentially lost funds.

To reduce operational and fraud risks, the Credit Union requires a separation of duties among Credit Union employees involved in ACH processing.

Center Parc has automatically enabled security alerts to send notifications when your password has been changed, or when an outgoing ACH transaction has been generated.

Please keep in mind that we will **NEVER** email you requesting your Cash Management password or token credential. We may on occasion call to verify other information regarding your on-line activity should we see something of concern in your login patterns.

## **WHAT HAPPENS IF A SECURITY BREACH OCCURS?**

Immediately contact the Credit Union if you suspect an ACH data breach. As an ACH Originator, you are required to immediately report the breach to the Credit Union who must report it to Nacha, NCUA and the Georgia Department of Banking & Finance.

## **CREDIT PUSH SCENARIOS**

### **BUSINESS EMAIL COMPROMISE SCHEMES**

Business email compromise schemes occur when the legitimate email account of a business officer is either compromised or impersonated and used to order or request the transfer of funds. An employee transfers funds to the fraudster believing the order was from a reputable company email address owned by an officer with authority to execute those orders.

#### **Prevention Tips:**

- 1) Verify all payments through a separate communication channel (phone, in person);
- 2) Implement dual-approval processes for high-value transactions; and

- 3) Educate employees to spot phishing tactics and unusual payment requests.

### **VENDOR OR SUPPLIER IMPERSONATION INVOICE FRAUD**

Vendor impersonation fraud occurs when a business, public sector agency or organization receives an unsolicited request, purportedly from a valid contractor, to update the payment information for that contractor. The fraudster is paid by the business, agency, or organization when the real contractor submits an invoice for work done or goods sold. Public sector organizations are frequently targeted because contact information is often in public record.

#### Prevention Tips:

- 1) Verify any changes to payment details with vendors directly.
- 2) Use trusted vendor portals for invoicing management instead of email-based instructions; and
- 3) Train employees to look for subtle changes in email addresses (e.g., 'supplies@abcdirect.com' versus 'supplies @abcdirect.com').

### **PAYROLL IMPERSONATION FRAUD**

Payroll impersonation fraud targets employees and human resources departments. A fraudster will impersonate an employee and contact the HR department directly or through the employer's payroll portal using stolen credentials. The fraudster requests to change the account where the employee's regular payroll is deposited. Once updated, the employer pays the fraudster rather than the employee.

#### Prevention Tips:

- 1) Require in-person or two-factor authentication (2FA) before making payroll changes;
- 2) Notify employees when their direct deposit details are updated; and
- 3) Monitor sudden multiple payroll updates from the same IP address.

### **DOUBLE-SIDED SPOOFING FRAUD**

Fraudsters simultaneously target both a business customer and their financial institution using spoofed phone calls and emails. They impersonate bank representatives or law enforcement to trick the business into revealing login credentials and security information. Using the stolen information, they then impersonate the business when contacting the financial institution, requesting a token reset or security override. Once the token is reset, they take over the business's account and initiated fraudulent ACH and wire transfers to accounts under their control.

#### Prevention Tips:

- 1) Verify independently, always call back at trusted phone numbers;
- 2) Require multi-factor or extra verification for token resets or profile changes;
- 3) Never share credentials, financial institutions will never ask for personal information over phone or by email;
- 4) Secure tokens and MFA devices;
- 5) Monitor accounts daily; and
- 6) Report suspicious activity immediately to the Credit Union

## **SOCIAL ENGINEERING FRAUD SCENARIOS**

### **WEBSITE SPOOFING**

Website spoofing occurs when fraudsters create a fake website designed to look identical to a legitimate site operated by a trusted business or organization. These spoofed websites trick individuals into entering sensitive information such as login credentials, account numbers, or payment details.

#### Prevention Tips:

- 1) Pay close attention to the website address (URL). A site may appear legitimate, but the URL may contain misspellings or use an unusual domain.
- 2) If you are suspicious of a website, close your browser and contact the company directly using a verified phone number or official site.
- 3) Avoid clicking links found on social media, pop-up windows, or non-trusted websites. Links can easily redirect you to spoofed sites. Typing the address directly into your browser is safer.
- 4) Only enter sensitive information on websites using a secure connection. Verify the URL begins with "https://" rather than "http://".
- 5) Do not use websites that trigger browser certificate warnings or security errors.

### **PHISHING**

Phishing is a type of fraud in which attackers pose as trusted individuals or organizations in electronic communications to steal sensitive information. Phishing attempts often direct victims to spoofed websites or prompt them to reveal credentials, financial details, or personal information. These attacks commonly occur through email, text messages (SMS), instant messaging, and telephone calls.

#### Prevention Tips:

- 1) Delete unsolicited emails or text messages that ask you to confirm or provide sensitive information. Legitimate companies will not request personal data through unsecured messages.
- 2) Be cautious when clicking website links sent via unsolicited communications.
- 3) Even if a message appears legitimate, manually type web addresses into your browser or use bookmarks instead of clicking embedded links.
- 4) Independently verify message details by contacting the company directly using trusted contact information.
- 5) Enable anti-phishing protections available in your email provider and web browser.

## **FILE DELIVERY DEADLINES & CUTOFF TIMES**

All transmissions to the Credit Union must be submitted by the established cutoff time of 4:00 PM Eastern Time in order to be processed on the same business day. Any transmission completed and received after this cutoff time, or on a non-business day, will be processed on the following business day.

Additionally, the Credit Union requires all ACH Originators to follow required security protections. For example, when responding to ACH Receiver requests to change account information, you must verify the request with a phone call to a trusted number already on file, not a number provided within an email request.

If you have questions about ACH or any of our Treasury Management products, please contact us at (800) 843-8491.

## BUSINESS DAYS & FEDERAL HOLIDAYS

ACH transactions are processed only on business days when the Credit Union is open; weekends and federal holidays do not count as processing days—see the holidays below.

Federal Holidays:	2026	2027	2028	2029	2030
<b>New Year's Day</b>	January 1	January 1	January 1*	January 1	January 1
<b>Birthday of Martin Luther King, Jr.</b>	January 19	January 18	January 17	January 15	January 21
<b>Washington's Birthday</b>	February 16	February 15	February 21	February 19	February 18
<b>Memorial Day</b>	May 25	May 31	May 29	May 28	May 27
<b>Juneteenth National Independence Day</b>	June 19	June 19*	June 19	June 19	June 19
<b>Independence Day</b>	July 4*	July 4**	July 4	July 4	July 4
<b>Labor Day</b>	September 7	September 6	September 4	September 3	September 2
<b>Columbus Day</b>	October 12	October 11	October 9	October 8	October 14
<b>Veterans Day</b>	November 11	November 11	November 11*	November 11**	November 11
<b>Thanksgiving Day</b>	November 26	November 25	November 23	November 22	November 28
<b>Christmas Day</b>	December 25	December 25*	December 25	December 25	December 25

\* Saturday - the Federal Reserve Banks are open, but the Board of Governors is closed on July 3, 2026, June 18, 2027, December 24, 2027, November 10, 2028, and December 31, 2028.

\*\* Sunday - the Federal Reserve Banks and the Board of Governors are closed on July 5, 2027, and November 12, 2029.

## **APPENDIX A**

### **ACTION ITEMS FOR NON-CONSUMER ACH ORIGINATOR FRAUD MONITORING**

#### **1. ORIGINATOR FRAUD-MONITORING PROCEDURES**

- Develop risk-based written procedures to identify potentially fraudulent originated ACH entries.
- Define methods to detect suspicious, abnormal, or high-risk activity.
- Document monitoring timing (post-processing, near-real-time, or periodic).
- Align monitoring cadence with organizational risk appetite.
- Clearly outline staff responsibilities.
- Incorporate Nacha's "False Pretenses" Definition into procedures. The inducement of a payment by a Person misrepresenting (a) the Person's identity, (b) that Person's association with or authority to act on behalf of another Person, or (c) the ownership of an account to be credited.
- Train staff to identify misrepresentations of identity, authority, or account ownership.

#### **2. DETECT UNAUTHORIZED OR FALSE-PRETENSES ENTRIES**

- Implement controls to reasonably identify unauthorized or False Pretenses Entries.
- Establish review steps to help employees recognize and flag activity that appears to be initiated under false pretenses.
- Investigate all indicators of unauthorized activity (misrepresentations of identity, authority, or account ownership) and document results.

#### **3. CONDUCT AND DOCUMENT OPERATIONAL MONITORING**

- Perform continuous monitoring of originated ACH Entries.
- Document all monitoring results, alerts, and review actions taken.
- Ensure monitoring is actively used – not merely written on paper.
- Maintain evidence demonstrating active monitoring.

#### **4. ANNUAL REVIEW OF FRAUD-MONITORING PROCESSES**

- Procedures must be reviewed annually for effectiveness and re-evaluated to address current fraud risks.
- Document findings, decisions, and improvement steps.

#### **5. UPDATE PROCESSES FOR EMERGING RISKS**

- Revise procedures when new fraud trends appear.
- Update procedures to reflect any operational changes and ensure staff are trained accordingly.

#### **6. MAINTAIN DOCUMENTATION FOR CREDIT UNION OVERSIGHT**

- Keep records of procedures, monitoring evidence, annual reviews, and risk-based controls.
- Provide documentation upon request.
- Retain for at least two years or longer if required by internal policy.

#### **7. MONITOR ALL ACH ENTRY TYPES**

- Apply fraud-monitoring controls to all originated ACH transactions.
- Document how monitoring covers each entry type.