See www.nachaoperatingrulesonline.org for the complete ACH Rules available for you to purchase.

****Annual ACH Security Review****

- You must maintain a signed authorization supporting all of your debit transactions and it must contain verbiage allowing for revocation (PPD).
- You must keep the signed authorization on file for 2 years after the termination or revocation of the authorization.
- If you use a website to obtain debit authorizations, the transaction is considered a WEB Standard Entry Class Code and must be properly formatted according to the Rules, including verifying Routing Numbers prior to initiating a live entry. Effective March 19, 2021, you must implement a fraudulent transaction detection system that must at a minimum validate the account number to be debited. Options include Prenotes at least 3 days prior to the live transaction being transmitted, Micro-Transactions, or other validation requests.
- · You must cease initiating entries if you have received any returns coded R07-Authorization Revoked, R08-Stop Payment, and R10-Customer Advises Not Authorized Originators, R29-Corporate Unauthorized; unless the receiver has re-instated his/her authorization or corrective action is taken. R11 Return code can be used to indicate that it was an authorized transactions, however there is an error with the debit entry.
- Any item (except RCK) may be re-initiated when the entry was returned for insufficient or uncollected funds; when the entry was returned due to stop payment and reinitiating has been separately authorized by the Receiver after the Originator/Originating Depository Financial Institution receives the Return, or the Originator/Originating Depository Financial Institution has taken corrective action to remedy the reason for the return.
    - Must be within 180 days of the original entry settlement date
    - Maximum of two additional attempts when returned for insufficient funds or uncollected funds
    - Re-initiated entries must be in a separate batch that contains the "RETRY PYMT" in the Company Entry Description of the Company/Batch Header Record
    - Contents of the Company Name, Company ID, and Amount fields must be identical to the contents of the original Entry.
- Fees associated with Returns must be in a separate batch that contains the Entry Description "Return Fee". Authorization language for Consumer debit requirements can be found in Article 2 subsection 2.14.2.
- You have 6 banking days or prior to initiating the next entry to correct entries that you have received a Notice of Change (NOC) or a return. You must maintain a copy of all NOCs received.
- You must notify Receivers when reversing entries will be originated no later than the settlement date of the reversing entry and you must provide the reason the original entry is being reversed.
- You may reverse an entry within five banking days of the effective date of the original entry. The batch header must contain "REVERSAL" in the company entry description.
- If you initiate prenotifications, you may not initiate live entries for three banking days after the effective date of the prenote.
- Upon receipt of returns relating to the prenote indicating that the RDFI cannot accept the entry, you should not initiate live entries.
- Same Day ACH transactions cannot exceed $100,000.00 (effective March 20,2020).
- Following Calendar year 2020, any originator that originates 2 million or more ACH transactions must protect account number data by rendering them unreadable when stored electronically and must be compliant by June 30th, 2021. This does not apply to paper document storage
- In the event Customer violates any of the applicable Rules and NACHA imposes a fine on Bank because of Customer's violation, Bank may charge the fine to Customer (up to $500,000) and revocation of PinnBank for Business privileges for noncompliance.
- You should have security procedures in place to mitigate the threat of Account Takeovers. These procedures should take in to account what is appropriate for your business, as well as identify your risk. The procedures may include:
    - Computer Security
    - Account Security
- Create a Security Framework Policy and Procedure that address the following:
    - How you protect the confidentiality and integrity of Protected Information
    - How you protect against anticipated threats or hazards to the security of Protected Information
    - How you protect against unauthorized use of Protected Information
    - How you educate your employees about your policies and procedures on Protected Information
    - Protect the confidentiality and integrity of Protected Information used to create or within an entry and any related Addenda Records.
    - Ensure Protected Information is protected against anticipated threats

- Protect against unauthorized use of Protected information that could result in substantial harm to a person
- *Account numbers must be protected by rendering them unreadable when stored electronically*

· When creating your policy and procedures, here are some questions that should be answered:
  - What type of information do you obtain – names, physical/email addresses, account numbers, bank routing numbers, tax id numbers, birthdates, types and amount of transactions?
  - How do you gather the information – paper, electronic, telephone, invoices, mailing lists (physical and/or email)?
  - How do you store this information – papers in a locked filing cabinet, saved to a password protected file, portable device like a USB?
  - Who has access to this information?
· You will notify bank of terminated employees who have PinnBank for Business Access.

You have been informed of ACH Rules and/or annual ACH Rules Revisions. **See www.nachaoperatingrulesonline.org for the complete ACH Rules available for you to purchase**

· Helpful links we encourage our clients to visit:
https://www.fbi.gov/scams-and-safety
http://www.epcor.org/docs/ach_security_framework_rlh/index.html