RESOLUTION 2026-02

A RESOLUTION ADOPTING THE CITY OF BROKEN BOW ACH ORIGINATOR POLICY AND PROCEDURES

WHEREAS, the City of Broken Bow (the "City") utilizes electronic payment methods through the Automated Clearing House (ACH) Network for efficient processing of disbursements and collections, including payroll direct deposits, vendor payments, utility collections, refunds, and other authorized transactions; and

WHEREAS, as an ACH Originator, the City must comply with the Nacha Operating Rules and Guidelines (the "Rules"), as administered by the National Automated Clearing House Association (Nacha), and with the terms of the Originating Depository Financial Institution (ODFI)/Originator Agreement with the City's financial institution; and

WHEREAS, compliance with the Rules requires the establishment of internal controls, proper authorizations, risk-based fraud detection procedures (including those mandated under 2026 amendments), secure transmission practices, employee training, and mechanisms to handle errors or unauthorized transactions; and

WHEREAS, the City has prepared the "City of Broken Bow ACH Originator Policy and Procedures" to define responsibilities, establish procedures, and mitigate risks associated with ACH origination, consistent with Nacha standards and best practices for municipal entities; and

WHEREAS, adoption of this policy by resolution will ensure uniform application across City departments, protect public funds, and demonstrate the City's commitment to regulatory compliance and fraud prevention;

NOW, THEREFORE, BE IT RESOLVED BY THE MAYOR AND CITY COUNCIL OF THE CITY OF BROKEN BOW, NEBRASKA, as follows:

1. **Adoption of Policy and Procedures**. The "City of Broken Bow ACH Originator Policy and Procedures," attached hereto as **Exhibit A** and incorporated herein by reference, is hereby adopted as the official policy governing all ACH origination activities by the City. All City officials, employees, and departments shall comply with its provisions.

2. **Effective Date**. This Resolution and the attached Policy shall take effect immediately upon passage and approval.

PASSED AND APPROVED this 24th day of February, 2026.

Rodney W. Sonnichsen, Mayor

ATTEST:

Jennifer A. Waterhouse, City Clerk

CITY OF BROKEN BOW CORPORATE SEAL NEBRASKA

EXHIBIT A

City of Broken Bow
ACH Originator Policy and Procedures

Purpose
The purpose of this policy is to define the City of Broken Bow's responsibilities as an ACH Originator and establish internal controls and procedures to ensure secure, compliant processing of ACH transactions. This policy is designed to reduce the risk of unauthorized activity and protect against ACH-related fraud.

ACH Originator Responsibilities
As an ACH Originator, the City of Broken Bow is required to comply with rules and guidelines for the creation, submission, and processing of electronic files. These rules are set by the National Automated Clearing House Association (NACHA), an organization which manages the development, administration, and governance of the ACH Network. The NACHA Operating Rules and Guidelines (the "Rules") can be accessed online at www.nacha.org. We acknowledge that failure to comply with the NACHA Rules can lead to termination of services and/or fines imposed by NACHA.

Key responsibilities include, but are not limited to:

- Complying with all requirements outlined in the ODFI/Originator Agreement with our financial institution
- Obtaining and retaining proper written authorizations for all ACH transactions
- Adhering to processing deadlines set by the Bank and NACHA
- Provide authorization records to the Bank upon request within NACHA's specified timeframes
- Safeguard all sensitive banking information
- Make necessary changes, as instructed from a Notification of Change (NOC), prior to the next ACH origination
- Ceasing subsequent entries when a Notification of Return is received due to administrative errors or unauthorized activity
- Discontinuing subsequent entries, when otherwise appropriate or when instructed by the Bank
- Maintaining secure computer systems and network environments in accordance with the ODFI/Originator Agreement with Bank.
- Implementing risk-based procedures to detect unauthorized payments, including those authorized under false pretenses
- Completing required ACH training and responding to any audit requests as required.

ACH Procedures
We acknowledge there are risks associated with originating ACH entries, and we are required to implement procedures to mitigate errors and the risk of unauthorized ACH

entries. Therefore, we will adhere to the following procedures when originating all ACH transactions:

- Authorization: A written, signed ACH authorization (for debits or credits) must be obtained and kept on file for each receiver. (e.g., utility payments, payroll).
- Authorization Verification:
    - New ACH authorizations will be confirmed using a secondary communication method (e.g., call back to a known phone number on file).
    - Any requested changes to ACH instructions will also be verified using a secondary communication method (e.g., call back to a known phone number on file).
- Secure Transmission: ACH files will be submitted through Internet Banking with multifactor authentication (MFA).
- Information Security: Sensitive banking data will be stored securely (e.g., in a locked cabinet/vault or secure server).

Handling Errors and Unauthorized Transactions

In the event of a suspected error or unauthorized ACH transaction, we will:

- Evaluate whether the transaction is the result of fraud, a scam, or an internal error
- Notify our financial institution immediately
- Contact law enforcement, if applicable
- Stop all future related ACH transactions

Employee Training and Awareness

Ongoing staff education is essential for mitigating ACH fraud risk. The following steps will be taken annually to ensure employees are informed about the evolving risks of fraud.

- Complete the required ACH Origination training provided by the Bank.
- Educate staff on current fraud schemes, including those delivered by email, phone, fax, or mail (phishing emails, phone impersonations, fraudulent mail).
- Train employees to recognize, question and independently authenticate changes in payment instructions, payment methods (e.g., ACH to wire) or pressure to act quickly or secretively.
- Respond to emails for payment requests using the "forward" option and type in the correct email address or select it from a known address book.
- Remind staff never to provide online banking login credentials or account information when contacted, even by your financial institution. Instead, hang up and call them via a known number.

Review

We will review this policy annually or upon significant changes in regulation or business practices.

Resolution Number: 2026-02

Date Approved By City Council: 2-24-26