ACH Origination Best Practices

Thank you for participating in First State Bank's ACH Origination program. ACH Origination is a convenient payment method, but it involves risks that must be reviewed regularly. As an Originator, you are responsible for understanding these risks and ensuring accurate processing. You must also have access to NACHA Operating Rules, available for free on their website. Review the following information to help maintain compliant ACH processing.

1. Comply with all U.S. laws, including requirements from the Office of Foreign Assets Control and Financial Crimes Enforcement Network, as well as applicable state laws.
2. Obtain written authorization for consumer entries and keep records for 2 years after they terminate.
3. Use prenotes to help ensure accuracy; correct any issues before sending live entries.
4. The bank will notify you of returns as soon as possible.
5. Stop entries if authorization is revoked unless corrected or reauthorized. Example: Returns coded R07 (Authorization Revoked by Customer), R08 (Payment Stopped) and R10 (Customer Advises Originator is Not Known or Not Authorized to Debit Receiver's Account).
6. Apply Notification of Change (NOC) updates within 6 banking days or before the next entry.
7. Notify receivers of reversals by the settlement date and explain the reason.
8. Use clear, standardized company entry descriptions to reflect the purpose of the payment (e.g., "PAYROLL," "PURCHASE").
9. Keep systems secure with up-to-date antivirus and software patches.
10. Train employees on security and incident response procedures.
11. Do not save login credentials; use strong passwords and update them regularly.
12. Limit ACH systems to business use only (no browsing or social media).
13. Monitor and reconcile accounts daily.
14. Keep security tokens safe and use dual control for ACH processing.
15. The bank may contact you through secure channels (e.g., online banking messages, secure file systems, mail, or phone). It will never ask you to click links, install software, share login credential, or change procedures without secure notice.
16. See **Appendix B** for examples of fraud attempts. If you notice suspicious activity or a possible breach, contact the bank immediately and follow your response plan **(Appendix C).**
17. See **Appendix E** for warning signs of a possible system or network compromise.
18. First State Bank Cortact Information:

    Mailing Address: PO Box 10, Gainesville, Texas 76241

    Street Address: 1818 N. Interstate 35, Gainesville, Texas 76240 Phone:940-665-1711

    Emergency Contact Information:

    Rachell Leach, AVP Treasury Management, 940-668-4300 ext 4234

    Nicole Calhoun, VP Treasury Management, 940-668-4300 ext 4712

    Lori Neu, Operations Systems Officer, 940-668-4300 ext 4186

For assistance or clarification on any of these items, please contact First State Bank at the contact information listed above.

Use trusted industry and agency resources (e.g., security publications and vendor sites) to stay informed-see **Appendix A.** For laws and regulations on safeguarding information, see **Appendix D.**

APPENDIX A- Business Resources

1. Better Business Bureau (Data Privacy)
2. U.S. Small Business Administration (SBA)
3. Federal Trade Commission (FTC) business data protection guide
4. Internet Crime Complaint Center (IC3)
5. Financial Services Information Sharing and Analysis Center (FS-ISAC)
6. NACHA website (fraud prevention and payment security resources)

APPENDIX B - Fraud Examples

1. The FDIC will not contact customers about ACH, wire transfers, account issues, or ask you to install software. Treat these messages as fraud and delete them-do not click links.
2. Messages from the IRS, Better Business Bureau, NACHA, or similar organizations asking for software, login details, or account information are likely fraud. Verify before taking any action.
3. Phone calls or texts requesting sensitive information are often fraudulent. Always verify using a trusted phone number from official records or websites, never use contact data that is provided in the message.

APPENDIX C - Incident Response Plan

Each business should create its own incident response plan. A basic plan should include:

1. Key bank contact information, including after-hours numbers.
2. Steps to limit fraud, such as:
    - Changing passwords
    - Disconnecting affected computers from online banking
    - Placing a temporary hold on transactions until verified
3. Information needed by the bank to help recover funds
4. Insurance carrier contact information
5. Coordination with computer forensic specialists and law enforcement if needed

APPENDIX D - Information Security Laws and Standards

Businesses are responsible for protecting sensitive data. Data breaches can lead to financial loss, reputational damage, and legal penalties.

Key Texas laws include:

1. Texas Business and Commerce Code Chapter 521 (Identity Theft Enforcement and Protection Act), including breach notification requirements and financial penalties.
2. Chapter 72, covering proper disposal of business records, including paper and electronic data.

Merchants that accept cards must also follow PCI Security Standards. Noncompliance may result in

fines, lawsuits, or loss of card processing privileges. Guidance is available on the PCI Security Standards Council website.

APPENDIX E - Signs of System Compromise

Watch for signs your system may be compromised:

1. Cannot access online banking
2. Slow computer performance
3. Screen changes or unusual display behavior
4. System freezing or locking up
5. Unexpected restarts
6. Unexpected one-time password or token requests
7. Strange pop-ups or "system unavailable" messages
8. New toolbars or icons
9. Cannot shut down or restart computer