Northeast BANK

ACH ORIGINATORS **FRAUD PREVENTION GUIDE**

This guide provides ACH Originators with best practices to protect against fraud, account compromise, and unauthorized ACH activity.

THE IMPORTANCE OF ACH FRAUD PREVENTION

ACH fraud can result in financial losses, operational disruption, and reputational harm to both the Originator and the Bank. Implementing strong internal controls and cybersecurity safeguards is essential to protecting your organization. ACH transactions are often targeted for fraud because of their speed and volume. Immediate reporting of suspicious or unauthorized activity is critical, as delays can limit recovery options and increase financial exposure.

Below is a common example of how quickly this can impact a business and why prevention is so important.

A company received an email from one of its vendors requesting updated ACH payment instructions due to a "banking system change." The employee updated the vendor record without verification. The next payment for $84,000 was sent to a fraudulent account.

BEST PRACTICES

INTERNAL CONTROLS FOR ACH ORIGINATORS

Strong internal controls dramatically reduce ACH fraud risk. Every ACH Originator should implement the following internal controls:

1. **Segregation of duties**
   Separate responsibilities ensure one individual does not control the entire ACH process.

   Recommended roles:
   - **File creator** – prepares the ACH file
   - **Approver** – reviews the file
   - **Release Authority** – transmits file to the Bank

2. **Dual Control**
   Require two authorized individuals to approve ACH batches prior to submission.

   Organizations should consider establishing limits for:
   - Maximum batch amounts
   - Maximum single transaction amounts
   - Number of transactions per batch

3. **ACH Positive Pay**
   The Bank currently offers ACH Positive Pay at no charge to our customers. This enhanced fraud solution allows you to provide a list of approved businesses that are allowed to debit your account electronically and return any that you do not approve.

VENDOR AND PAYMENT CHANGE VERIFICATION

Fraudsters frequently target businesses that originate ACH transactions by impersonating their vendors. Originators can significantly reduce their fraud risk by considering the following when changing any ACH payment instructions.

- Never rely solely on email instructions. Call-back verification should always be required.
- Independently verify the request using a known phone number.
- Require documentation from the vendor that supports the change.
- Require approval for vendor bank changes and maintain that approval documentation after changes are made.
- Conduct periodic monitoring for unusual payment activity.

CYBERSECURITY

Many ACH fraud events start with compromised computers or stolen credentials. ACH Originators should consider implementing the following cybersecurity safeguards to protect their data:

1. **Use Dedicated ACH Workstations**
   Whenever possible, submit ACH files from a computer used only for online banking activities.

2. **Multi-factor Authentication**
   Ensure all users accessing ACH services use multi-factor authentication (MFA).

3. **Patch and Update Systems**
   Keep operating systems, browsers, and security software up to date.

4. **Avoid Public Wi-Fi**
   Never submit ACH transactions using public or unsecured networks.

5. **Strong Passwords**
   Require complex passwords and avoid reusing credentials across systems.

EMPLOYEE AWARENESS

Fraudsters often target employees directly. To protect your organization, employees involved in ACH processing should receive training on the following scams and their warning signs.

1. **Phishing and email scams**
   - Unexpected emails asking you to log in to a system
   - Messages creating urgency such as "your account will be locked"
   - Email links that don't match the official website
   - Attachments from unknown senders

2. **Vendor impersonation scams**
   - Vendors requesting immediate banking changes
   - Requests to send payments to new accounts or unfamiliar banks
   - Emails stating that previous payment instructions are no longer valid

3. **Social engineering attacks**
   - Requests for sensitive information over the phone
   - Pressure to act quickly without verification
   - Requests to bypass security controls

4. **Business email compromise (BEC)**
   - Urgent payment requests from executives
   - Slight changes in email addresses or domain names
   - Emails asking employees to bypass normal procedures

5. **Payroll diversion fraud**
   - Unexpected requests to change direct deposit
   - Requests submitted through email instead of normal HR systems

6. **Account takeover**
   - Login alerts from unfamiliar locations
   - Unrecognized system users
   - Unusual ACH batches or transaction amounts

KEY TAKEAWAYS

Most fraud attempts succeed not because criminals are sophisticated, but because internal controls are weak or bypassed. Protecting ACH transactions requires a combination of:

1. **Strong internal controls**
2. **Cybersecurity safeguards**
3. **Employee training**
4. **Timely monitoring**

INCIDENT RESPONSE

If you suspect fraud or unauthorized ACH activity, take the following actions:

1. **Contact the Bank immediately – late reporting can limit recovery options**
2. **Disable affected user credentials**
3. **Preserve relevant emails or logs**
4. **Notify internal management and/or your IT staff**