ConnectOneBank
a better place to be

Nacha Fraud Risk Program Guide

Monitoring ACH transactions prior to processing provides the greatest opportunity for detecting potential fraud. The adoption of proactive measures prior to the origination of entries can help stop the transmission of fraudulent entries. Because fraud monitoring applies to all types of ACH transactions, it may be appropriate to conduct a risk assessment as a first step, taking into account the nature, types, and scope of the risks those originations present to your enterprise.

A risk-based process does not require every ACH entry to be screened individually. Instead, it allows ACH participants (financial institutions, originators, and other parties) to focus resources where risk is higher, applying enhanced monitoring and controls to elevated-risk transactions while using standard controls for lower-risk activity.

As a starting point to develop risk monitoring practices and procedures, consider a review of current practices and procedures to identify risk and fraud controls they may already have in place and to formalize those practices and procedures, as needed.

- Consider whether existing monitoring could be expanded to adopt or improve.
- The identification of anomalies in volume and value of ACH payments originated, including the frequency and velocity of payments to the same account number or the same Receiver name on accounts.
- Return entry monitoring and analysis to identify anomalies on origination.
- Account validation prior to first use of an account number for any ACH payment, regardless of whether it is a credit or a debit.

Fraud Threats

As fraud schemes continue to grow and evolve, it is critical that an Originator understand the nature of those fraud schemes and adopt appropriate risk control measures to combat them.

Commonly Used Terms

Used in the discussion of various fraud schemes:

Malware: Malicious software, including viruses, ransomware, and spyware, designed to damage systems, disrupt operations, or gain unauthorized access to data.

Money Mule: An individual who transfers or moves illegally obtained funds on behalf of a fraudster. Fraudsters often recruit money mules to help launder proceeds from fraudulent activity.

Social Engineering: The use of deception or manipulation to trick individuals into providing confidential or personal information.

Spear-phishing: Targeted emails that appear to come from a known or trusted sender, intended to trick the recipient induce the recipient into revealing sensitive information.

Spoofing: The act of disguising an email or communication so it appears to come from a known, trusted source when it actually originates from an unknown or fraudulent sender.

False Pretenses, Unauthorized Entries and Other Disputes

The term "**False Pretenses**" refers to the inducement of a payment by a person misrepresenting (a) that 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. For example, False Pretenses covers the following fraud scenarios:

- Business Email Compromise (BEC)
- Vendor impersonation
- Payroll impersonation
- Other payee impersonations

"False Pretenses" does not cover scams involving fake, non-existent, or poor-quality goods or services. Payment made to the right person but induced on a fraudulent basis is not considered to have been made under False Pretenses. The term "False Pretenses" complements language on "unauthorized credits" (i.e., account takeover scenario), but entries made under False Pretenses are not "unauthorized."

Examples of credit entries authorized by you (the Originator) under False Pretenses:

- The Receiver of the credit Entry misrepresents the Receiver's identity or ownership of the receiving account.

- A fraudster impersonates someone with the authority to order payment (e.g., a CEO/CFO via business email compromise) to induce someone with authority to originate a payment from your company's account.
- A fraudster claims to be a real estate settlement agent or attorney and requests funds transferred to the fraudster's account.
- A fraudster claims to be a vendor with whom the business has a relationship with and requests payment to a "new" account that would instead credit the fraudster's account.
- A fraudster claims to be an employee of an organization and requests payment to the fraudster's account; or fraudster gains access to the employee-facing component of an organization's payroll system and redirects payroll payments to the fraudster's account.
- A fraudster claims to be a governmental agency (e.g., IRS) claiming a person is delinquent in payment (e.g., taxes) with consequences if not paid.
- A fraudster claims to be the company's bank and tells the Originator that their account has been compromised and to avoid losses, they need to move their funds to another account that has been opened for them.

Examples of Unauthorized Credit Entry:

- Account takeover- Fraudster gains access to the credential necessary to initiate a credit transaction from the accessed account.

Common Fraud Schemes

Business Email Compromise

With Business Email Compromise, legitimate business email accounts are either compromised or impersonated, and then used to order or request the transfer of funds. The fraudster will often compromise on the business' officers and monitor his or her account for patterns, contacts and information. Using information gained from social media or "out of office" massages. The fraudsters will often wait until the officer is away on business to use the compromised email account to send payment instructions. After identifying the target, ploys are conducted such as spear-phishing, social engineering, identity theft, email spoofing, and the use of malware to either gain access to or convincingly impersonate the email account. Payment instructions direct the funds to an account controlled by the fraudster or a money mule.

Vendor Impersonation Fraud

Vendor Impersonation Fraud can occur when a business, public sector agency, or organization (example: a municipal government agency, a school district, etc.) receives an unsolicited request. Purportedly from a legitimate vendor or contractor, to update or change payment information or change payment method. The update could be new routing and account information for ACH or wire payments, or a request to change the payment method from check to ACH or wire payment. This type of request could come from fraudsters and not the vendor or contractor. Although any business entity could be the target of this type of social engineering attack, public sector entities may be specifically targeted because their contracting information is often public record.

Payroll Impersonation Fraud

Payroll Impersonation Fraud occurs when a fraudster targets an employee by sending a phishing email that impersonates the employee's human resources or payroll department and/or the company's payroll platform. The email directs the employee to log in to confirm or update payroll information, including bank account information. The employee clicks the link or opens the attachment within the email and confirms or updates the payroll information. The fraudster then uses the stolen login credentials to change payment information to an account controlled by the fraudster or a money mule.

Debit Origination

When originating debit entries, be aware of the potential for abuse of or fraud schemes involving payments authorized more than the amount owed by the Receiver. Originators are encouraged to implement processes and procedures to limit or prohibit the acceptance/authorization of overpayments.

See **Procedure/Program Guide** section for a list of suggested internal controls to help fight against fraud attacks.

Procedure/Program Guide

NACHA does not prescribe a specific format for risk-based procedures. More importantly, an ACH fraud monitoring program should be tailored to your organization's structure, payment volume, and unique fraud risks. Our dedicated webpage also outlines key components to consider, which can help you develop a procedure that fits your needs.

For more information, visit our website at:

https://www.connectonebank.com/insights-and-resources/upcoming-nacha-changes

Procedure Framework/Template

The following format is only a sample to help structure your risk procedures. These can serve as a starting point and can be built upon as needed.

- Purpose
- Scope
- Systems & Access
- Roles & responsibilities
- ACH Origination Process
- Transaction Monitoring Procedures
- Fraud Prevention Controls
- Return & Notification Handling
- Incident Response
- Annual Review & Updates
- Documentation & Record Retention

Controls Framework

Demonstrate a proactive risk-based approach

- **Dual Authorization/Segregation of Duties:** Require at least two separate individuals to authorize high-dollar payments or ACH files. No single person should be able to create, approve, and release payment.
- **Vendor Payment Information:** When receiving an email, phone call, fax or mailed letter request for a bank account change (vendor or employee), verifying the change via a trusted secondary channel (e.g., a phone call to a known number on file, not the number listed in the suspicious email).
- **System Controls and Anomaly Detection:** Utilizing your internal accounting or payment systems to automatically flag or alert you to unusual activity, such as:
    - Payments to a new vendor that exceeds a set dollar threshold
    - Sudden increases in transaction volume or amount outside of normal business patterns
    - Unusual payment destinations (e.g., high-risk geographical locations)
- **Pre-Payment Account Validation:** Utilizing ACH prenotes (zero-dollar verification) or third-party validation services to confirm the existence and ownership of a new vendor's or employee's bank account before the first live payment is initiated
- **Strong Access Controls (MFA):** Limiting the number of employees who have access to your ACH origination system and enforcing Multi-Factor Authentication (MFA) for all users to protect against compromised login credentials
- **Dedicated Payment Workstations:** Restricting the computers used to initiate or approve ACH payments from being used for high-risk activities like opening external email attachments or general web browsing
- **Formal Fraud Incident Response Plan:** Maintaining a clear, documented plan that specifies the immediate steps to take if fraud is detected, including who at ConnectOne Bank to call and internal protocols for isolating the risk
- **Mandatory, Continuous Employee Training:** Implementing regular (e.g., quarterly) training for all staff involved in payments to recognize, question, and independently authenticate suspicious requests (a key defense against social engineering).
    - Employees should not provide or post nonpublic business information on social media.
    - Do not use the "reply" option when authenticating emails for payment requests. Instead, use the "forward" option and type in the correct email address or select from a known address book. Or for suspected phishing emails, forward it to a company security contact.
    - Alert employees to watch for phishing attacks and suspicious malware links.
    - Instruct employees to not enter their login credentials when clicking on a link or opening an attachment in an email.

- **Routine and Red Flag Reporting** – Review and reconcile accounts daily. Generate regular reports that identify transactions to new relationships, transactions of existing customers to new accounts, or abnormal activity. Verify that these transactions were intentional.
- **Review User Rights** – Review user rights to online banking systems regularly and promptly remove access for terminated or transferred employees who no longer require access.
- **Secure Systems and Applications** – Ensure maintenance of firewalls and make sure antivirus software is up to date. Ensure all system components and software have the latest vendor-supplied security patches installed.
    - Avoid free web-based email accounts for business purposes. A company domain should always be used in business emails.
    - To make impersonation harder, consider registering domains that closely resemble the company's actual domain.

Establishing an effective ACH fraud risk management program is an ongoing responsibility that requires continuous monitoring, periodic review and alignment with evolving risks. While this guide outlines key considerations and best practices. Each Originator is responsible for developing and maintaining controls appropriate to their specific operations, transaction activity, and risk profile.

As your ODFI (Originating Depository Financial Institution), we remain committed to supporting your efforts through guidance, collaboration, and oversight. We encourage you to periodically review your processes, update controls as needed, and reach out to the Bank with any questions or for further assistance in strengthening your fraud risk management framework.