Fraud Monitoring

Recommendations for implementing risk-based processes and procedures

adelfi

Better banking. Higher purpose.

Table of Contents

False Pretenses

- Term that refers to the inducement of a payment by a person misrepresenting:
  - Person's identity
  - Person's association with or authority to act on behalf of another person
  - The ownership of an account to be credited
- Covered Fraud Scenarios:
  - Business Email Compromise
  - Vendor or Payroll Impersonation
- False pretenses does not cover scams involving fake, non-existent, or poor-quality goods or services. A payment made to the right person but induced on a fraudulent basis is not considered to have been completed under false pretenses. This type of scam is not considered to be "unauthorized".

False Pretenses Continued

Examples of entries authorized by an Originator under False Pretense:

- Receiver of a credit entry misrepresents the receiver's identity or ownership of account
- Fraudster impersonates someone with authority to order payments to induce another with origination authority to initiate/create a payment
- Fraudster claims to be one of your vendors and requests payment be made to the fraudster's account
- Fraudster claims to be a government agency (IRS) claiming a person is delinquent in a tax payment and there will be consequences if not paid
- Fraudster claims to be the ODFI (your financial institution) and advises your account has been compromised and to avoid losses you will need to move your funds to another account that has been opened for you
- Fraudster gains access to an employee-facing component of the payroll system and redirects payroll payments to a fraudster's account

An unauthorized entry is when the account holder did not authorize the entry to be initiated. An example of an unauthorized entry would be account takeover – fraudster gains access to the credentials necessary to initiate a transaction from the accessed account.

Risk-Based Fraud Monitoring

Monitoring transactions prior to processing provides an Originator the opportunity to detect potential fraud.

- Return rate monitoring
    - R04 – Invalid Account
    - R03 – No Account/Unable to Locate
        - Stop further processing for these receivers
        - Consult receiver, using previously verified communication method, to determine validity of transaction
- Review for anomalies in the volume and value of ACH batches – look for frequency of entries to the same account number and receiver name
- Account Validation prior to first use of an account number (prenote)
- Require a second person to confirm and release ACH batches

Understanding Fraud Threats

Key Terms commonly used for various fraud schemes:

- Malware – Malicious software including viruses, ransomware, and spyware, typically consisting of code designed to cause extensive damage to data and systems or to gain unauthorized access.
- Money Mule – Someone who transfers or moves illegally acquired money on behalf of a fraudster. Fraudsters recruit money mules to help launder proceeds derived from many of the fraud schemes discussed in this presentation.
- Social Engineering – The use of deception to manipulate individuals into providing confidential or personal information.
- Spear-phishing – Sending emails supposedly from a known or trusted sender to induce the recipient to reveal confidential information.
- Spoofing – Disguising an email from an unknown source as being from a known, trusted source.

Common Types of Cyberfraud Schemes

- Business Email Compromise – legitimate business email accounts are compromised or impersonated and then used to order or request the transfer of funds.
  - A fraudster will compromise a business officer's email account and monitor his/her account for patterns, contacts and information. The fraudster will gain information from social media or "out of office" messages and wait until the officer is away on business and use the compromised email account to send payment instruction.
    - A fraudster conducts spear-phishing, social engineering, identify theft, email spoofing and the use of malware to either gain access to or convincingly impersonate the email account.
- Internal Controls:
  - Attacks can come via email, phone call, fax or letters in the mail.
  - Recognize, question and independently authenticate changes in payment instructions, payment methods or pressure to act quickly or secretively
  - Verbally authenticate any changes via a telephone call using a previously known number
  - Review accounts frequently
  - Initiate payments using dual controls
  - Never provide password, username, authentication credentials or account information when contacted
  - Do not post nonpublic business information on social media
  - Avoid free web-based email accounts for business purposes
  - Do not use "reply" for emails – use "forward" and manually type the correct email address or select from a known address book

Common Types of Cyberfraud Schemes - Continued

- Vendor Impersonation Fraud – Occurs when a business, public sector agency or an organization receives an unsolicited request, supposedly from a legitimate vendor or contractor, to update or change payment information or payment method.

- Internal Controls:

  - Attacks can come via email, phone call, fax or letters in the mail.
  - Recognize, question and independently authenticate changes in payment instructions, payment methods or pressure to act quickly or secretively
  - Verbally authenticate any changes via a telephone call using a previously known number
  - Review accounts frequently
  - Initiate payments using dual controls
  - Do not post nonpublic business information on social media
  - Do not use “reply” for emails – use “forward” and manually type the correct email address or select from a known address book
  - Make vendor payment forms available via secure means or to known entities
  - Require changes to payment information be made or confirmed only by site administrators and use methods like the transmission of verification codes to existing contracts
  - Do not ignore calls from a financial institution questioning the legitimacy of a payment

Common Types of Cyberfraud Schemes - Continued

- Payroll Impersonation Fraud – fraudster targets an employee by sending a phishing email that impersonates the employee's human resource or payroll department or the company's payroll platform.
  - Email directs the employee to log in to confirm or update payroll information, including account information. Employee clicks on the link or opens the attachment in the email and confirms or updates the payroll information. Fraudster then uses stolen login credentials to change payment information to an account controlled by the fraudster or money mule.

- Internal Controls
  - Alert employees to watch for phishing attacks and suspicious malware links
  - Direct employees to check the actual sender email address, rather then just looking at the subject line, to verify the email came from their employer or payroll service provider
  - Educate employees not to reply or respond to any suspicious email, instead, have them forward the email to a company security contact
  - Instruct employees to not enter their login credentials when clicking on a link or opening an attachment in an email
  - Employer self-service platforms should authenticate requests to change payment information using the employee's previously known contact information – require a second password that is emailed to an existing email address or use a hard token code
  - Employer self-service platforms should re-authenticate users accessing the system from unrecognized devices, using the employee's previously known contact information
  - Set up alerts when banking information is changed or multiple changes using the same new routing number or an identical account number
  - Validate new account information by using prenotes, Micro-entries or other account validation service

General Controls for Payment Origination

Proactive measures Originators can put into place prior to initiating entries to help minimize the potential for transmitting erroneous, unauthorized, or potentially fraudulent entries:

- Authenticate the requester
- Confirm the validity of the authorization
- Verify the account number and routing number of the Receiver
- Confirm the effective date of the transaction
- Confirm any payment-related information
- Confirm there are sufficient funds in the funding account
- Obtain required internal approval for the transaction
- Require a second person to confirm and release the transaction

ACH Originator Fraud Monitoring Compliance

Per Nacha (National Automated Clearing House Association) Rules:

- No later than June 19, 2026, all ACH Originators must be compliant with fraud monitoring.
- ACH Originators must establish and implement risk-based processes and procedures that are reasonably intended to identify entries that are suspected of being unauthorized or authorized under False Pretenses.
- ACH Originators must review their processes and procedures and make appropriate updates to address evolving risks on an annual basis
- See Chapter 15 – Originator Risk Management in the ACH Rulebook for more information

AdelFiBanking.com
800.634.3228

135 S. State College Blvd, Suite 500
Brea, CA 92821

adelfi
Better banking. Higher purpose.