ACH RISK MANAGEMENT REQUIREMENTS FOR FRAUD MONITORING

Who Must Comply?	What is the Requirement?
Non-Consumer Originators, Third-Party Senders and Third-Party Service Providers performing functions of ACH processing on behalf of one of these entities	Establish and implement risk-based processes and procedures to identify payments suspected of being **unauthorized or authorized under "false pretenses."**

An **unauthorized** payment would result if a fraudster compromised your company's online banking login credentials (e.g., captured by malware, convinced you to share) and then initiated a payment unbeknownst to you. An **authorized under false pretenses** payment refers to the inducement of a payment by a person misrepresenting themselves. Through social engineering, like urgency or sense of importance, a fraudster convinces a person to initiate (authorize) a credit payment to their account. These fraud schemes include business email compromise, vendor impersonation, payroll impersonation and other payee impersonation. And each involves a cybercriminal creating fake emails that appear to be from legitimate senders, like CEOs, vendors or employees.

When Does the Requirement Become Effective?	
No later than March 20, 2026:	**No later than June 19, 2026:**
Non-consumer Originators, Third-Party Senders and Third-Party Service Providers whose annual ACH Origination or transmission volume exceeded 6 million entries in calendar year 2023.	All other non-consumer Originators, Third-Party Senders and Third-Party Service Providers, regardless of origination or transmission volume must be compliant.

What is Risk-Based Fraud Monitoring?

Risk-based processes and procedures do not require screening of individual ACH payments, nor do they need to be automated processes. A risk-based approach allows your company to apply resources and take extra measures to identify and detect fraud. While the *ACH Rules* do not prescribe what your company's risk-based approach should be, having **no monitoring in place is not acceptable**.

The intent of this new requirement is for your company to identify payments suspected of being unauthorized or authorized under false pretenses. It does not impose an obligation on your company to prevent wrongful activity. Simply, the expectation is to do your best to detect fraud and keep those payments from being processed into the ACH Network.

Regardless of your company's size, you can easily determine if an email request you receive is legitimate or not by taking the following actions:

STOP	THINK	VERIFY
Take a breath. Don't react immediately.	Think with your head and not with your heart. Does this seem like a valid request?	Contact sender request to confirm its validity of email request whether in person, via a phone number you have on file, or by "forwarding" the email to an email address in your contacts list.

The following list of considerations is not all inclusive nor is it one-size fits all. Your company's risk-based processes and procedures for detecting fraud should be unique to your organization and its payments activities.

Originating Company Considerations
Implement procedures to protect against account takeovers and other fraud schemes.
Educate staff on current fraud schemes originating via email, phone calls, faxes or mailed letter.
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.
Remind staff to never provide online banking login credentials or account information when contacted, even by your financial institution.
Verify account information associated with first-time payments (e.g., ACH prenotes, micro-entries).
Initiate payments using dual controls.
Review your accounts frequently (i.e., at least daily).

Beyond monitoring, your company ought to be prepared to take steps should you detect fraud (e.g., reporting to designated personnel, notifying your financial institution or law enforcement). And you should annually review your fraud monitoring processes and procedures and update, as needed, to address evolving fraud risks.

Prepare Now
Implement, or update, risk-based processes and procedures to identify and detect fraudulent transactions.
Set a reminder to review your fraud monitoring processes and procedures annually and update, as needed, to address evolving fraud risks.
Contact your financial institution to better understand the new requirement and to learn about their risk-based processes and procedures related to fraud monitoring.
Develop processes for reporting fraudulent activity.