

SOUTHERN MICHIGAN BANK & TRUST

ACH Origination Risk Management and Assessment Tool

Section 1: Company Information

Understanding your company profile is key to assessing and controlling the risk associated with ACH activity. Consider your company's annual ACH volume and value, the type(s) of ACH payments you conduct, the strength of your processing procedures and the controls already in place.

Company Name:	
Prepared By:	
Date Completed:	
Annual ACH Volume (#):	
Annual ACH Dollar Value (\$):	

Section 2: Inherent Risk Assessment

Inherent risk is the level of fraud risk your organization is exposed to based on the nature of your ACH activity, including factors such as transaction volume, dollar amounts, payment types, operational complexity, and industry risk. Every organization has a baseline level of risk based on how it uses ACH before any controls are applied. This section is intended to help you identify the risk associated with ongoing ACH activity. Rate each category and provide rationale. Do not default to "Low" without explanation—your rating should reflect how your ACH program operates.

1. Select **Low**, **Moderate**, or **High**
 - **Low:** Limited exposure; simple operations; predictable activity
 - **Moderate:** Moderate exposure; some complexity or variability
 - **High:** Significant exposure; complex, high volume, or fraud-prone environment
2. Record a short explanation of the selected rating.

Risk Category	Rating (L/M/H)	Score (1–3)	Explanation
ACH Volume	Low – Limited number of transactions; predictable activity; typically single use case (e.g., payroll only) Mod – Regular recurring files; multiple payment types (e.g., payroll + AP); moderate growth or seasonal spikes High – High transaction volume or rapid growth; multiple business units/files; may approach or exceed Nacha high-volume thresholds		
Dollar Exposure	Low – Small-dollar payments; limited financial exposure if fraud occurs Mod – Moderate dollar ranges; potential for noticeable financial impact High – High-dollar transactions or large aggregate exposure; single file could result in material loss		

SOUTHERN MICHIGAN BANK & TRUST

ACH Origination Risk Management and Assessment Tool

Section 2: Inherent Risk Assessment (continued)

Risk Category	Rating (L/M/H)	Score (1–3)	Explanation
Payment Types	Low – Limited to one payment type; low-risk use cases (e.g., internal transfers or stable payroll) Mod – Mix of payment types (e.g., payroll + vendor ACH credits) High – Broad mix including higher-risk categories (e.g., consumer debits, online payments, refunds, third-party processing)		
Change Activity	Low – Infrequent changes; controlled through centralized process Mod – Periodic updates (vendors/employees); some decentralization High – Frequent or decentralized changes; multiple staff can update payment instructions		
Initiation Method	Low – ACH files initiated internally with limited, controlled access Mod – Mix of local and remote access; controlled but broader user base High – Fully remote/cloud-based initiation; multiple users, API integrations, or third-party platforms		
Third-Party Involvement	Low – No third-party processors Mod – Limited vendor involvement (e.g., payroll provider) High – Multiple third parties (TPS/TPSP), fintech integrations, or acting on behalf of others		
Industry Risk	Low – Industry not typically targeted for ACH fraud Mod – Some exposure to vendor payments or customer refunds High – High-risk sectors (e.g., construction, healthcare, staffing, property management, fintech, marketplaces)		
Transaction Variability	Low – Stable, predictable payment patterns Mod – Occasional fluctuations in timing or amounts High – Irregular activity, spikes, or significant variation in amounts, recipients, or timing		
Total Risk Score	Low – 8 to 12 Moderate – 13 to 18 High – 19+		Low - Basic controls, manual monitoring Moderate - Formal procedures, monitoring thresholds High - Enhanced monitoring, automation, formal

Section 3: Fraud Risk Exposure

Fraud risk exposure refers to the specific types of fraud your organization may encounter based on how you originate ACH transactions, including both unauthorized transactions and payments made under false pretenses. Understanding how different types of fraud could impact your business is essential to designing meaningful controls. Evaluate your ACH activities against these common fraud techniques. List the controls in place to mitigate inappropriate ACH origination due to fraud.

Fraud Type	Definition	Current Controls
Business Email Compromise (BEC)	A fraud scheme in which a criminal impersonates a trusted individual (e.g., executive, vendor, or employee) via email (or similar communication) to trick a business into initiating an ACH payment to a fraudulent account.	
Vendor Payment Diversion	A fraud scheme where a criminal poses as a legitimate vendor and convinces a business to update payment instructions, redirecting ACH payments to an account controlled by the attacker.	
Payroll Redirection	A fraud scheme in which a criminal alters employee direct deposit information, so payroll funds are sent to an unauthorized account.	
False Pretenses (social engineering)	A transaction that appears authorized but only occurred because the sender was deceived.	

Describe any gaps identified as part of this review:

Section 4: Control Inventory

These controls represent commonly used safeguards to help organizations comply with Nacha requirements to maintain risk-based processes for identifying and preventing ACH fraud. Controls should be tailored to your organization's size, complexity, and risk profile and should match your operations. List the controls currently in place.

Control and Definition	Enforced?	Description of Use
Dual Control – a control requiring two separate individuals to release a payment	☐	
Callback Procedures – a process to independently verify payment instructions or changes using a trusted contact method	☐	
ACH Limits – predefined transaction, batch, or daily dollar limits on ACH activity	☒	The Bank enforces transactions limits on ACH activity.
Vendor Verification – process to validate the identity of a vendor and confirm the accuracy of payment instructions prior to making a payment	☐	
User Access Controls – controls that restrict and manage user access to ACH systems based on job responsibilities	☐	
Exception Reporting – use of reports, alerts or system-generated notifications to identify transactions that fall outside normal activity	☐	
Other (describe)	☐	

Describe any gaps identified as part of this review:

Section 5: Fraud Monitoring Procedures

Fraud monitoring procedures are the processes your organization uses to review ACH transactions and identify potentially fraudulent activity, based on your risk profile. These are the ongoing checks and reviews you perform to catch suspicious activity, like unusual transaction amounts, changes in payment behavior and new or modified payees. Your response should reflect how you actively identify suspicious activity.

Describe how ACH transactions are monitored for fraud:

Monitoring Components	Description
Describe the monitoring method employed at your business. Is it manual or automated?	
When does transaction monitoring occur?	
What are the thresholds or triggers for additional scrutiny on a payment?	
How often are transactions reviewed?	
Are specific personnel dedicated to completing the monitoring and escalating for additional review?	

Describe any gaps identified as part of this review:

Section 6: Escalation Process

Detecting suspicious activity is only effective if there is a clear and timely response. Consider the steps your organization follows when potential fraud or suspicious ACH activity is identified, including internal review and communication with SMBT or related financial institutions.

Explain what happens when something looks suspicious:

Escalation Components	Description
What happens when something looks suspicious?	
Who is notified internally?	
Who is notified externally?	
How do you determine whether to stop transactions?	

Describe any gaps identified as part of this review:

Section 7: Annual Review

ACH risks and fraud methods continue to evolve, so controls must be reviewed at least annually or as your ACH activity changes.

Last reviewed date:	
Last reviewed by:	
Description of changes:	