SALTMARSH, CLEAVELAND & GUND

Saltmarsh
Saltmarsh, Cleaveland & Gund
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

May 6, 2024

Risk in the ACH Function

J. Michael Maricelli, CIA, CISA, AAP

CONTACT

J. Michael Maricelli, CIA, CISA, AAP

Senior Consultant, Financial Institutions

michael.maricelli@saltmarshcpa.com

(225)-571-6255

(800) 477-7458

Saltmarsh

Saltmarsh, Cleaveland & Gund

CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Saltmarsh, Cleaveland & Gund

ABOUT THE FIRM

Saltmarsh is one of the largest locally-owned CPA and business advisory firms in the Southeast, serving clients throughout the U.S. and worldwide from offices across Florida and in Nashville, Tennessee.

SIZE OF FIRM

OFFICE LOCATIONS

5

FLORIDA
Destin
Orlando
Pensacola
Tampa

TENNESSEE
Nashville

AFFILIATIONS

SALTMARSH FINANCIAL ADVISORS, LLC
Saltmarsh
Financial Advisors, LLC
AN AFFILIATE OF SALTMARSH, CLEAVELAND & GUND

THE BDO ALLIANCE USA
AN INDEPENDENT MEMBER OF
BDO
ALLIANCE USA

Saltmarsh
Saltmarsh, Cleaveland & Gund
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

SERVICES OFFERED

Audit & Assurance | Business Valuation | Financial Institution Consulting | Financial Planning | Flexible Spending Plan Administration | Healthcare Consulting | Human Resources Consulting | Information Technology Consulting | Investment Management | Litigation & Dispute Advisory | Managed IT Services | Outsourced Accounting Solutions | Research & Development Tax Credits | Retirement Plan Administration | Tax Compliance & Consulting

OUR CLIENTS

Community Banks | Construction & Real Estate Development | Credit Unions | Governments, Municipalities, Special Districts & Pension Plans | High Net Worth Individuals | Hospitality | Manufacturing & Distribution | Non-Profit Organizations | Post-Acute Healthcare | Professional Employer Organizations | Technology & Emerging Growth

saltmarshcpa.com | (800) 477-7458

Agenda:

- **What is ACH**
- **Why is a risk assessment and why do one for ACH**
- **Areas to include in an ACH Risk Assessment**
- **Questions**

Questions & Comments at ANY TIME

*DISCLAIMER: The information presented here or stated by the speaker(s) or others at Saltmarsh is **not to be considered legal advice nor a replacement for reading the applicable statute, regulation, official interpretation, commentary, supplemental information, or regulatory guidance or publication** related to the subject matter discussed or contained herein. Not all state or payment rules are addressed (i.e., wire transfers under UCC).*

Saltmarsh
Saltmarsh, Cleaveland & Gund
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

4

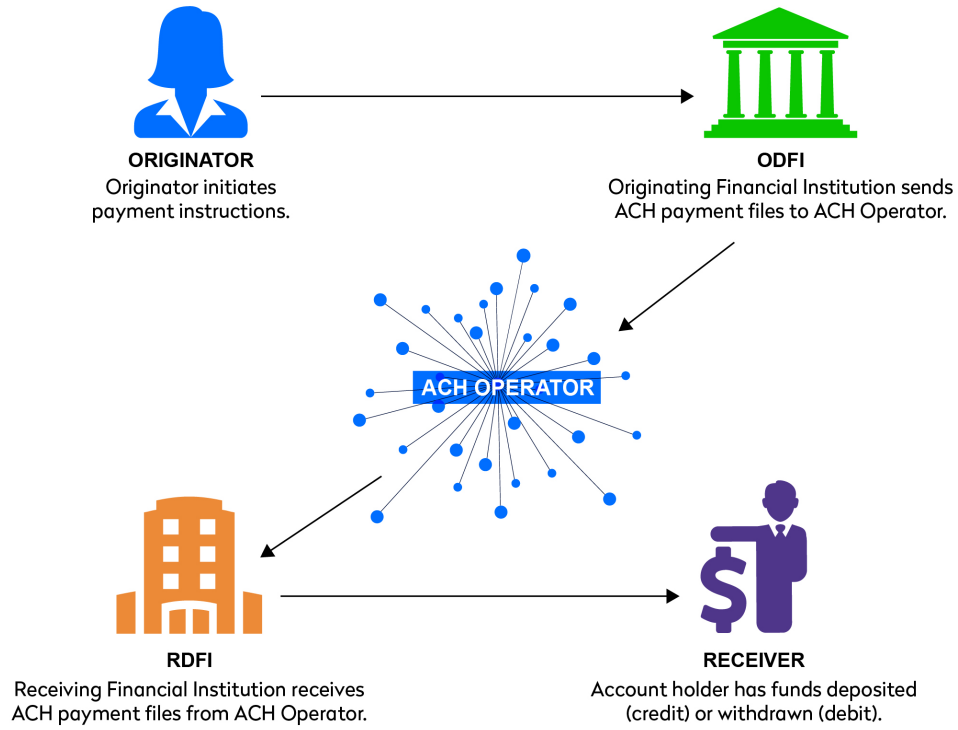
Cash May Be King, But ACH IS Still Royalty

ACH is:

- An electronic funds transfer;
- Debits and Credits transferred between Banks and Credit Unions across the Automated Clearing House Network;
- In 2022, there were 30 billion ACH Network payments valued at $77 trillion.

Saltmarsh
Saltmarsh, Cleaveland & Gund
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

How ACH Payments Work



- Originator – Person (P2P) or Company (utility company or fitness center)
- ODFI – Loan payments on its on behalf; debits or credits for its customers (ex. Membership dues or payroll)
- RDFI – Payroll deposits and accounts receivable payments for customers; credits for loan payments held by the Bank
- Receiver – Payroll deposits and accounts receivable payments; membership fees; loan payments

ACH Risk Assessment: It's Required!!!

The ACH Network is governed by Nacha:

- **N**ational **A**utomated **C**learing **H**ouse **A**ssociation
- Annual publication of the Nacha Operating Rules & Guidelines.

Article One Subsection 1.2.4 Risk Assessments states a participating DFI and Third-Party Sender must:

- Conduct, or have conducted, an assessment of the risks of its ACH activities;
- Implement, or have implemented, a risk management program on the basis of such an assessment; and
- Comply with the requirements of its regulator(s) with respect to such assessment and risk management program.

Regulatory Guidance

- Nacha Operating Guidelines, Section 1, Chapter 4, Risk Assessments:
  - Generally, regulators stress the importance of **1)** assessing the nature of risks associated with ACH activity; **2)** performing appropriate know-your-customer due diligence; **3)** establishing controls for Originators, third-parties, and direct-access to ACH Operator relationships; and **4)** having adequate management, information and reporting systems to monitor and mitigate risk.
  - Examples of recent risk-management requirements and guidance by regulators can be found on the Nacha website at: https://www.nacha.org/content/regulatory-guidance .

Risk Assessment

- Start by considering inherent risk, the combination of internal and external risks in their pure, uncontrolled state.
- Identify controls in place to reduce or eliminate risk.
- Determine whether residual risk remaining after elimination or reduction of risk by controls is within the company's risk appetite.

Risk Assessment (Cont.)

- Risk Assessment is a systematic process of identifying, analyzing, and evaluating the potential risks that may be involved in an activity or undertaking.
- Risk Assessment should be at the center of a typical risk management process.

Areas to Include and Review in the ACH Risk Assessment

1. Governance and Oversight
2. Independent Reviews
3. Compliance Risk
4. Credit Risk
5. Operational Risk
6. Disaster Recovery and Incident Response Plans
7. Information Technology and Information Security
8. Corporate Origination
9. Third-Party Senders

Saltmarsh
Saltmarsh, Cleaveland & Gund
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Message from the Captain

Governance and Oversight

Ensure the Board and senior management establish clear roles and responsibilities for ACH governance and oversight, including oversight committees, senior management involvement, and periodic reviews of ACH risk management practices.

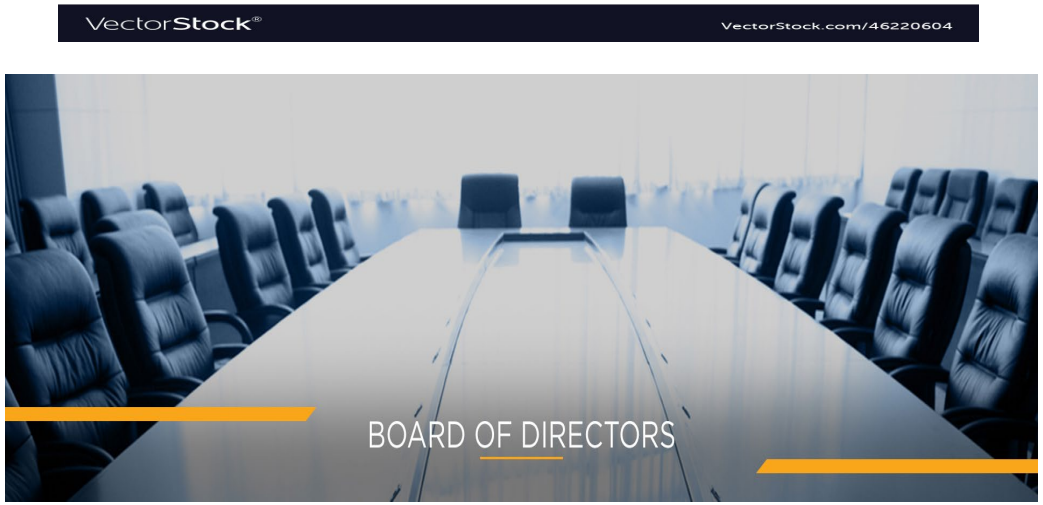
Board of Directors Involvement

- ACH Policy
  - Define the scope of ACH activities
    - Receiving
    - Originating
    - Acceptable/Prohibited SEC Codes
- Periodic Reports
  - Metrics and tend analyses on ACH volume, returns, operational losses, and transaction types;
  - Summary of returns rates by originator, and third-party senders;
  - Financial reports on profitability of the ACH function as a cost center.

Senior Management Involvement

- ACH Procedures
  - Step-by-step processes to implement the Board approved activities and controls to reduce risk to Board approved tolerances
- Daily/Weekly/Monthly Reports on ACH activity

13



Saltmarsh
Saltmarsh, Cleaveland & Gund
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Independent Reviews (Audit Program)

An effective audit program and scope should consider the volume and complexity of the auditee's ACH operations, including new or expanded products and services. Attention should be given to new ACH systems, underwriting policies and customer due diligence policies and procedures, and customers' online access to ACH products and services.

While the Nacha Rules Compliance Audit is an important part of compliance within an ACH Program, it is NOT a substitute for a risk-based audit.

An effective audit function should be staffed with auditors who have sufficient expertise to evaluate all aspects of the ACH Program.

- Certified Internal Auditor (CIA)
- Accredited ACH Professional (AAP)
- Accredited Payments Risk Professional (APRP)

Compliance Risk

Assess adherence to regulations such as the Nacha Rules and relevant laws like the Electronic Funds Transfer Act (Reg. E), the Bank Secrecy Act (BSA), Anti-Money Laundering (AML), and Office of Foreign Assets Control (OFAC)

Nacha

- ACH Audit
  - Has the financial institution had an ACH Audit prior to December 31 or the prior year?
  - Does the ACH Policy require completion of an ACH Audit annually by December 31?
- Record Retention
  - Are ACH policies, procedures, risk assessments, audit findings, authorizations, and records of ACH transactions being maintained in accordance with Bank retention policies and Nacha Rules?
- Training
  - Does the financial institution provide training on ACH rules to appropriate staff?
  - Does the financial institution encourage employees to obtain relevant certifications (Ex. AAP, APRP)?

Regulation E/Unauthorized Entries

- Does the financial institution have documented procedures for the handling of entries disputed by customers as unauthorized or revoked authorization?
- Training
  - Does the financial institution provide training on ACH rules to appropriate staff?
  - Does the financial institution encourage employees to obtain relevant certifications (Ex. AAP, APRP)?

Compliance Risk (Cont.)

OFAC

- Does the financial institution Originate IAT entries?
  - Is an OFAC check required on originated OFAC entries? Is this process manual or automated?
- Does the financial institution run an OFAC check on in-coming IAT Entries? Is this process manual or automated?
- Are there written procedures detailing steps to be taken of an outgoing or incoming IAT entry has a positive OFAC hit?

BSA

- Does the BSA/AML/Anti-Fraud monitoring solution include ACH transactions from all channels?
- Does the BSA officer understand the system settings for the BSA/AML/Anti-Fraud Monitoring solution
- Customer Identification Program (CIP)
  - If the financial institution uses third-party senders, does the third-party sender perform CIP on the companies they originate payments for?

Credit Risk

Assess the risk a party to a transaction will be unable to provide the necessary funds for the settlement of the transaction.

Credit Origination

- ACH credit origination presents **funding risk.**
- Funding risk is the risk that the originator will have funds in its account when the effective date of the transaction occurs.
- Originators can transmit credit entries into the network up to two business days prior to the effective date of the transaction.
- When the ODFI sends the credit entries to the ACH Operator, the ODFI warrants that the origination has been done in accordance with the Rules.
- If the Originator does not have funds in the account on the effective date of the transaction, the ODFI is responsible to the Network for those transactions.
- ODFI's can consider **prefunding**, taking the funds from the Originator's account at the time the transactions are originated, as a way of limiting risk.
- Origination limits should be tailored to the individual originator's needs. Limits should be high enough to comfortably conduct business, while low enough to limit exposure to the bank. (Ex. If originator is processing internal payroll, consider enough room to allow for a third payroll processing per month twice per year based on a 26 pay period schedule)

Credit Risk (Cont.)

Debit Origination

- For ACH debit entries, the ODFI incurs credit risk from the time it grants its customers funds availability until the ACH debit can no longer be returned by the RDFI.

Debit Origination Controls

- Underwriting standards that provide for a rigorous analysis of the originators' creditworthiness;
- Appropriate exposure limits;
- Holdbacks or reserve accounts and Lines of Credit accounts;
- Periodic reviews: Originators' financial condition and exposure limits should be reviewed on an ongoing basis. Circumstances change and that means risk changes.

Operational Risk

Assess risks such as human error or computer mishaps that may delay or alter ACH transactions.

Common controls include:

- Documented ACH processing procedures;
- Documented, up-to-date Business Continuity and Disaster Recovery Plan with regular testing;
- Ongoing training for employees involved in the ACH function.
  - IT Security Training (Phishing Tests)
  - Accredited ACH Professional (AAP)
  - Accredited Payments Risk Professional (APRP)
  - Continuous improvement process to learn from disaster recovery testing, audit findings, industry developments

Third-Party (Vendor) Risk

Evaluate and assess the financial institution's compliance, credit, and reputation risks by using third parties in ACH transactions.

The financial institution remains legally responsible but does not have direct control over the functions performed by the third party.

Common controls to reduce third party risk include:

- Board approved Third-Party (Vendor) Management Policy;
- Documented procedures that address due diligence requirements in deciding to outsource functions and selecting vendors; contract requirements and reviews, ongoing monitoring, and contingency plans.

Disaster Recovery and Incident Response Plans

Assess the financial institution's ability to respond to and recover from various weather, pandemic, and cyber related events.

Control procedures include:

- Does the institution have a Business Continuity Plan and Incident Response Plan?
  - Is the plan reviewed regularly by appropriate personnel?
  - Do employees receive training on recovery processes?
- Review institutions Business Impact Analysis (BIA)
  - Are ACH activities and required systems identified in the BIA?
  - Are recovery time objectives (RTO's) and Recovery Point Objectives (RPO's) properly classified in accordance with the criticality of the function?
  - Are the RTO's and RPO's for ACH activities and required systems in alignment?
- Review prior testing scenarios
  - Did testing include ACH activities?
  - Was testing adequate to determine whether recovery processes would be effective?
  - Were failures documented, remediated, and retested to ensure functionality?

Information Technology and Information Security

Assess the financial institution's controls over the technology used to provide ACH services.

Controls should be in place to ensure only those individuals with a need to access ACH related systems have access. Access levels should be within approved risk tolerances and provide for segregation of duties and dual control when possible.

Common control processes include:

- Approved procedures for granting and modifying system access;
- Ensuring dual control features are activated and functioning when available;
- Dollar limits on approval authority of ACH files;
- Restrictions on who has "override" authority;
- System access reviews;

Information Technology and Information Security (Cont.)

Common control processes include:

- Customer access – Dual control should be utilized in the approval and setup of customers. Additionally, non-consumer customers should be responsible for approving user access and notifying the institution when access should be modified. Dual control on the customer side should be utilized when permitted in the system;
- Data Security – Are procedures in place to ensure data received from customers and transmitted by the financial institution are secured? Does the financial institution have procedures to identify confidential and/or critical data used in ACH operations and ensure proper storage, retention, and disposal of such information?

Corporate Originators

Determine whether the institution permits non-consumer customers to originate ACH entries on behalf of receivers.

Common risks include:

- Credit risk – funding risk and return risks
- Fraudulent entries (rogue employees)
- Business email compromise
- Compliance risks (proper authorizations and retention of authorizations)
- Reputation risk

Corporate Originators (Cont.)

Common controls include:

- Agreed upon processes for transmitting files to the financial institution in the appropriate format by the agreed upon timeframe;
- Origination agreements that state the financial institution is authorized to follow any and all instructions entered, and transactions initiated using applicable and agreed upon security procedures unless and until the customer has notified the financial institution the security procedures or security device has been stolen, compromised, or otherwise become known to persons other than the users;
- Periodic testing of originators retention of authorizations (particularly for higher risk SEC codes such as TEL or WEB);
- Extensive underwriting and approval process prior to granting access to ACH origination;
- Procedures to ensure approved exposure limits (dollar amount and SEC codes) are what is entered into the system.

Third-Party Senders

Third-party senders act as an intermediary on behalf of an originator or another third-party sender in transmitting entries between the originator and the ODFI (or the ACH Operator on behalf of the ODFI via Direct Access), when there is not an originator agreement between the originator and ODFI.

- Third-party sender must have an originator agreement with an ODFI or another third-party sender.
- A third-party sender is never the originator for entries it transmits on behalf of another organization.
- TPS are Bank customers to which originators outsource payment services, and the Bank has no direct customer or contractual relationship with the originator.

Third-Party Senders (Cont.)

Third-Party Sender Controls:

- At a minimum, the Bank should know for which originators third-party senders are initiating ACH entries into the network:
  - The Bank should require TPS's to provide information on their originators such as the originator's name, taxpayer ID number, principal business activity, and geographic location;
  - The Bank should verify the originator is operating a legitimate business.
- Greater scrutiny during onboarding of third-party senders:
  - Does the TPS use more than one Bank to originate transactions or are they moving Banks? Be cautious if TPS's are changing Banks. Don't be afraid to ask "Why?"
  - Ongoing review of the TPS's financial condition with corresponding adjustments of exposure limits and required prefunding or collateral accounts.
- Written agreements

Third-Party Senders (Cont.)

Written agreements should:

- Define the information that must be provided to the Bank before the third-party sender can submit transactions for a new originator;
- Detail the obligations and liabilities of the third-party sender;
- Define approved and disallowed originator and transaction types;
- Provide the Bank ongoing access to all originators' files;
- Outline the Bank's right to audit such files and/or third parties so that the Bank can verify the third-party sender's compliance with Bank policies.

Join our Facebook group, "Saltmarsh Bank Talk"

Join a Saltmarsh User Group for virtual networking and best practices!

Sign up at www.thebankadvisors.com

Saltmarsh
Saltmarsh, Cleaveland & Gund
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS