Managing Third Party Risk in the ACH Network

Tony DaSilva, AAP, CISA
Senior Examiner
Federal Reserve Bank of Atlanta

Paul A. Carrubba
Partner
Adams and Reese LLP

THIS PRESENTATION IS DESIGNED TO PROVIDE ACCURATE AND AUTHORITATIVE INFORMATION REGARDING ITS SUBJECT MATTER.

IT IS PRESENTED WITH THE UNDERSTANDING THAT THE PRESENTER IS NOT RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES.

IF LEGAL ADVICE OR OTHER EXPERT ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT.
Learning Objectives

- Understand the risks associated with Third-Party relationships
- Understand risk mitigation best practices and requirements
Third-Party Processor
Third-Party Sender
*NACHA Operating Rules*
Regulatory Guidance
Case Study
Best Practices
Risk Management
Conclusion
What is a Third-Party Processor (TPP)

- A company that is contracted, by a bank etc., to conduct some part of a financial transaction process; especially a company that provides software or hardware for such a process.
- A party which processes ACH files and/or items on behalf of one of the participants in the ACH system.
What is a Third-Party Sender (TPS)

A third-party service provider is considered to be a third-party sender when there exists an agreement with an ODFI or another third-party sender to originate transactions and also has an agreement with an originator to initiate transactions into the ACH Network on their behalf.
Examples of TPS

- Payroll Company
- ACH Processing Company
- Remotely Created Checks
COLLECT YOUR PAYMENTS ON TIME: With EFT there is no more waiting for the payment – you submit the transaction files and your customer’s bank accounts are debited exactly on time. And you receive complete and detailed reporting on each and every transaction.

ONE TIME OR RECURRING: The system is designed to enable a business to collect their payments from their office – you can collect one time payments, recurring payments, weekly, monthly – you name it.

TELEPHONE PAYMENTS: Our clients love to use our telephone payment system. Just take your customer’s payment information over the phone and submit a debit through our web based system – the funds are take out of the customer’s account the next morning.
About ACH Direct, Inc.

ACH Direct is one of the fastest-growing privately held electronic funds transfer processors in the United States. ACH Direct's customers benefit from a comprehensive suite of payments products and services, including ACH origination, check verification, identity verification, credit card and debit card processing. Dedicated to providing superior customer service and industry-leading technology, ACH Direct provides tools to help organizations of all sizes reduce transaction costs, mitigate risk and increase efficiencies.
Risk?

- Third-Party Processors
- Third-Party Senders
- Direct Senders
Risks

- Credit (Pre-funding, reserve requirements, debit vs. credit origination)
- Transaction (Technology)
- Fraud
- Regulatory & Compliance
- Reputational
Are all Third Party Senders High Risk?

NO!

However, they present a higher level of risk.
The Risk Management and Assessment rule requires that all Participating DFIs conduct a risk assessment of their ACH activities and implement risk management programs based on the results of such assessments, in accordance with the requirements of their regulator(s). Generally, regulators stress the importance of assessing the nature of risks associated with ACH activity, performing appropriate know-your customer due diligence, establishing controls for Originators, third parties and Direct Access relationships and having adequate management, information and reporting systems to monitor and mitigate risk.
ODFIs are also impacted by the requirements to conduct additional risk management practices prior to originating ACH entries and cover specific topics in their Originator and Third-Party Sender agreements. The impact depends on the nature and complexity of each ODFI's ACH activity. ODFIs that do not conduct similar risk management practices or those that need to revise their Originator agreements will be the most affected. Requirements to modify Originator and Third-Party Sender agreements apply to those entered into or renewed after June 18, 2010. There is no requirement to modify agreements in place before June 18, 2010.
This rule provision outlines certain rights that ODFIs have related to their Originators and Third-Party Senders including:

- the right to terminate or suspend an Originator, or any Originator of a Third-Party Sender, or the Third-Party Sender for breach of the Rules; and

- the right to audit an Originator's, or Third-Party Sender's and its Originators', compliance with their agreement with the ODFI and the Rules.
The amendment expands the annual rules compliance audit requirement to include Third-Party Senders within its scope. To the extent that a Third-Party Sender performs any functions of an ODFI under the *Rules, it must also meet the audit requirements that are otherwise applicable to the ODFI.*

Under the *Rules,* each ODFI that enters into an agreement with a Third-Party Sender for the transmission of entries remains responsible for the Third-Party Sender’s performance of various obligations under the *Rules.* As with other provisions of the *Rules,* an ODFI will be responsible for its Third-Party Sender’s completion of a rules compliance audit. However, similar to the existing *Rules compliance audits for* Third-Party Service Providers, this amendment will not require an affirmative obligation on the part of an ODFI to verify that its Third-Party Senders have conducted the audit.
ODFIs are required to address their rights to terminate or suspend, audit, and place restrictions on ACH origination activity within any new or renewed agreement with their Originator or Third-Party Sender. There are no new restrictions on origination activity prescribed in this rule provision. Each ODFI is required to address its internally-developed restrictions on origination, if any, within its Originator and Third-Party Sender agreements so as to highlight the importance, and improve the enforcement, of such restrictions.
ODFIs are required to perform a more comprehensive set of risk management practices in addition to the current *Rules* on exposure limits.

These requirements include performing due diligence with respect to Originators and Third-Party Senders sufficient to form a belief that the party has the capacity to perform its obligation in conformance with the *Rules*, assessing the nature of the Originator's or Third-Party Sender's ACH activity and the risks it presents, establishing procedures to monitor the Originator's or Third-Party Sender's origination volume and return activity, relative to its exposure limit, across multiple settlement dates and enforce the exposure limit, and establishing procedures to enforce restrictions on the types of ACH transactions that may be originated.
Requirements reflect ACH industry best practices, send a strong message to the industry on the importance of risk management, ensure that all ODFIs perform know-your-customer due diligence and establish procedures, systems and controls to manage the risks of their Originator's and Third-Party Sender's ACH activities.
Regulatory Guidance

- FFIEC Retail Payment Systems IT Examination Handbook, February 2010
- OCC Bulletin 2008-12, Payment Processors, April 24, 2008
- FFIEC Guidance on Risk Management of Remote Deposit Capture, January 14, 2009
A third-party relationship should be considered significant if the institution's relationship with the third-party is a new relationship or involves implementing new bank activities; the relationship has a material effect on the institution's revenues or expenses; the third-party performs critical functions; the third party stores, accesses, transmits, or performs transactions on sensitive customer information; the third-party markets bank products or services; the third party-provides a product or performs a service involving subprime lending or card payment transactions; or the third-party poses risks that could significantly affect earnings or capital.
The institution’s management should ensure that appropriate procedures are in place, taking into account the complexity and risk potential for each of its third-party relationships. The precise use of a risk management process is dependent upon the nature of the third-party relationship, the scope and magnitude of the activity, and the risk identified.
Case Study

- A $200 million asset Community Bank with little or no payments experience
- However, a large ACH Originator of **Debits** and **Credits**
- Using a Third-Party Processor
- Who is also a Third-Party Sender and a Direct Send Fed Processor
- An agreement with a Third-Party Sender whose ACH volume is 100% TEL & WEB to process through their primary Third Party Sender
- ACH Fees are Significantly Over Market Price
Volume slow at first
Picks up quickly and at peak approximately 20% of bank’s income
Running Multiple Originators (Businesses) through one account
Significant wire activity including international wires (Incoming & Outgoing)
Internal transfers and wires between over 50 deposit accounts
Transfers from Business to Personal Accounts (cash)
The Issues

- The lure of significant Fee Income and Deposits
- Lack of Experience
- Lack of Adequate Due Diligence
- Lack of Board and Senior Management Oversight
- Poor monitoring of activity
- Inadequate BSA/AML Training
- Failure to address the obvious NACHA Operating Rules issues
- Failure to adequately address Consumer Complaints
- Failure to submit SARs on Obvious Suspicious Activity
Types of Originators

- Most companies in business one to two months
- Credit Card offers to poor credit customers
- Travel Packages
- Offshore Prescription Drugs
- Cigarettes
- Offshore Gambling
- Adult Entertainment
- Fix your Credit Problem Offers
- Companies located in Canada, Costa Rica,....
- ETC.......................
30% to 40% Return Rates
Customer Complaints
FBI & FTC Freeze all Bank Accounts
FBI & FTC Raid Third Party Senders Building
TPS President – Prior Federal Convictions
Organized Crime Ring
Bank Cited for Numerous BSA & AML Violations
Red Flags

- High levels of customer complaints:
  - Loss of key customer business
  - Increases in customer complaints and unauthorized returns
  - Breaches in internal service level agreements
  - Lawsuits
  - Customers complain for a reason
    - Understand the nature of the complaints and look for patterns
    - How did management respond to the complaints?
    - How quickly did management resolve the complaints?
Lack of written policies, procedures, **exposure** limits:
- Absence of these often indicates sloppy or inexperienced management
- Lack clear authorities

High or increasing number of failed transactions or returns:
- Look for reports of returns **by customer**, failed transactions, or payments that fail to settle
- These may indicate staff problems, spikes in business volumes, system problems
Due Diligence, Due Diligence….

- Know Your Customer
- Know Your Customer’s Customer
- BSA/AML
- Background Checks
- Credit – D&B (Financial Analysis)
- References (prior bank)
- Terminated File
Specific TPS Agreement that includes:

- *NACHA Operating Rules* & Applicable Regulations
- TPS and Originator comply with U.S. Laws
- Credit Approval
- TPS must perform Due diligence on Originator
- TPS complies with Security Requirements of the Rules
- Bank’s right to require Agreement with Originator
- Bank’s right to audit TPS and Originator
- Obligations of Third-Party Sender
  - Perform all duties including duty to Identify Originator
  - Assume responsibilities of Originator
  - Make all warranties and representations
  - Indemnification for action of Originator
  - Audit
- Establishes Limits
- Pre-Funding
- Reserves
- Termination Clause
Financial institutions can mitigate many of the risks associated with electronic payments origination & processing:

- Based on a comprehensive risk assessment of the financial institution’s electronic payments environment
- Board and management oversight that establishes appropriate risk tolerances, effective reporting, employee training, and prudent vendor management practices
- Leverage Existing Risk Management Processes
- Involve those Risk Management Professionals in the ACH Risk Management Effort
- Incorporate ACH into Broader Payment Risk Management Program
Risk Management Overview - FFIEC

Applicable Risk Categories:

- Credit Risk
- Compliance/Legal Risk
- Settlement Liquidity Risk
- Reputation and Strategic Risk
- Operational – Systems and Technology
- Operational – Internal Controls and Fraud
Bank’s Risk Culture:

- What is the FI’s payment strategy (risk taker vs. risk averse)?
- Does the bank have a disciplined and consistently followed process for initiating, analyzing, and approving new products and services (prior to rolling out)?
- Does the FI pursue relationships with high-risk merchants or merchant processors?
- Does the FI enforce strict risk limits set by the Board?
- Is compliance with policies and controls monitored and enforced?
Bank Management Knowledge and Skills:

- What level of knowledge does senior management demonstrate regarding retail products offered?
  - Inherent product risks?
  - Compliance requirements and ability to monitor?
  - Operations management and operational risks?
  - Reputational?
  - Legal?

- How deep is the management across the product lines? Subject Matter Experts?

- Does management ensure retail payments strategy matches with overall strategy and competencies of the entire bank?
**Customer Selection:**

- What is volume and volatility of ACH lines not set up for prefunding?
- Do customers have sufficient business experience and sophistication?
- Are customers and third parties financially strong?
- Does ACH activity expose the bank to risks from specific industries?
- Does customer selection integrate concerns from other risk management functions in setting risk limits and scope of due diligence (ERM, Audit, IT, Credit Admin)?
**Complexity of Retail Payments Products:**

- What retail and commercial payment products are offered?
  - ACH products such as BOC, RCK, POP, WEB, TEL, IAT?
  - Does the bank offer mobile banking and mobile payments?
  - Does the bank offer contactless cards?
  - Does the bank offer stored value cards?
- Does bank offer new products and services in addition to well established products?
- Is the bank a first-to-market leader with retail payment products?
- Does bank personnel and expertise align with payment channels and product offerings?
ACH Risk Management and Mitigation

**Common Risk Management Issues:**

- ACH/payments risk management not sufficient for scope of activities (informal, decentralized, or missing)
- Anxiety for income combined with passive oversight of third-party sender or originator activity
- Insufficient policies and expertise for the complexity
- Lack of adequate customer due diligence/underwriting for exposure to credit or legal liability losses
- Lack of effective oversight over third party senders
- Limited Board and senior management involvement
- Insufficient risk monitoring and MIS
- Inadequate *NACHA Operating Rules*, BSA/AML, or consumer protection training
ACH Risk Management Methods:

- Policies, standards, and risk limits
- Underwriting, due diligence, & oversight
- ACH agreements
- Transaction limits and controls
- Risk monitoring and MIS
- Audit and Control Testing
ACH Risk Mitigation

Primary Risk Mitigation Tools (MIS)
– Consider frequency, audience, timeliness

Lower Risk and Lower Volume
- Track daily, multi-day exposure limits
- Track ACH volume and return trends and compare to capital
- Identify and track customer-specific originations and returns (risk-based and/or volume-based threshold)
- Identify and track highest risk ACH originators
- ACH originator list with SEC code restrictions, limits, ACH line review date, and agreement date
- Track ACH over limits and exceptions

Higher Risk and Higher Volume
- All from lower risk plus:
  - ACH originations and returns by debits, credits, SEC type, third-party sender, originator
  - Track ACH reserve adequacy
  - High-risk ACH originator risk ranking report
  - High-risk ACH, tracking returns by SEC types and return code
Credit Risk can be mitigated by:

- Thorough credit and financial analysis for originators, third party vendors, & third party senders
- Ensure ACH agreements are maintained & updated
- Ensure policy includes a list of prohibited and high risk originators and SEC codes w/ approval process
- Establish risk-based debit and credit limits w/ exception approval requirements
- Effective customer activity monitoring and reporting
- Establish appropriate pre-funding and reserve requirements
Mitigate Compliance and Legal Risk by:

- Implementing comprehensive BSA/AML, KYC, GLBA, and OFAC screening policies and procedures
- Conducting due diligence for unfair and deceptive practices by originators and third party senders (e.g., FTC Telemarketer Rule)
- Conducting adequate monitoring of 3rd parties to ensure effectiveness of due diligence and monitoring processes
- Performing required audits and independent reviews
- Ensuring that all origination agreements and third party contracts contain regulatory and compliance language
- Ensuring proper monitoring and exceptions reporting
- Ensuring that employees have the proper training - AAP
ACH Risk Management and Mitigation

*Mitigate Liquidity Risk by:*

- Monitoring ACH volumes and trends
  - Identifying peaks in usage
  - Tracking volatility in payments activity
  - Assessing impact on funding

- Use of prefunding and reserves to limit additional funding requirements

- Using expiration dates for higher ACH limits for increased seasonal or temporary needs

- Identifying deposit concentrations from payment processing activity and assessing related volatility as a source of funds
Mitigate Reputational and Strategic Risks by:

- Conducting background checks on originators and third-party senders
- Expanding oversight of high-risk originators
  - NACHA Operating Rules
  - Due diligence and risk management program
  - Consumer complaints and litigation
  - Regulatory actions
  - Marketing and business practices
Mitigate Operational Risks from Systems & Technology by:

- Establishing comprehensive vendor management program
- Establishing and monitoring effective service levels
- Ensuring daily monitoring and reporting of any issues
- Ensuring that employees have the proper training and expertise - AAP
- Ensuring appropriate access controls, authentication, separation of duties, and independent control reviews
- Ensuring consistent internal controls and processing procedures across multiple technology applications and platforms
- Ensuring adequate contingency plans and testing
- Performing adequate audits with NACHA Operating Rules as starting point
Mitigate Operational Risk from Fraud by:

- Ensuring proper due diligence including background checks
- Using fraud detection software to filter suspicious activity
- Verification/validation of transmission
- Strict adherence to credit and other related policies
- Ensuring that credit originators require pre-funding or more in-depth financial analysis and underwriting
- Ensuring appropriate limits are in place
- Establishing adequate reserves for debit originators
- Complying with NACHA and Operator rules/regulations
- Requiring and enforcing updated agreements for all originators and third-party senders
- Monitoring activity and exceptions reports on a daily basis
Planning
- Clearly defined objectives, well-developed business strategy, clear risk parameters, role w/in FIs strategic plan

Risk Identification & Assessment
- Incorporate into existing risk management process, will vary by institution, non-public personal info. & third-parties

Mitigation & Controls
- Policies & procedures, clearly defined responsibilities, strong internal controls over transactions, risk-based audit program, well designed agreements

Measuring & Monitoring
- Periodic reports allow board to determine activities remain w/in board established risk parameters
Is the bank’s board knowledgeable and capable of understanding the risks

Determine if the quality of staffing levels are adequate
- Reports showing staffing levels, turnover, trends
- Level of skill
- Staffing levels for peak periods
- Adequacy and quality of staff resources
  - **AAP**
There is adequate capacity for current and planned transaction volumes

Automated vs. manual processes

Quality of controls
  - Separation of duties
  - Dual control
Policies should include:

- Goals and objectives of the program
- Approved ACH products
- Prohibited Originators
- Third Party Senders
- Exposure limits and Originator review
- ACH Agreements
- OFAC, PATRIOT Act, BSA/AML
ACH Policies (cont.)

- UCC4A provisions
- Third Party Service Providers
- Direct Access to the ACH Operator
- File Delivery
- Data Breach
- ACH Audit
Review Originator Agreements

- Do the agreements adequately set forth the responsibilities of all parties?

- Do the agreements contain the requirements of the *NACHA Operating Rules*?

- Do the agreements mention funding arrangements, SEC codes allowed, Regulation CC, UCC 4A, and Regulation E?
Non-Contractual Relationship with Originators

Need a specific contract to address risks

- Contract should include:
  - ODFI approval of all originators
  - Exposure limits per originator
  - An exposure limit for the TPS
  - Method to identify each originator

Third-party sender audit now required
Vendor Management

- Assess management’s ability to manage outsourced relationships with technology service providers
  - Encrypt transactions while in route between service provider and institution
  - Contract provisions
    - Personnel, equipment,
  - Contingency planning
- Measurements specify what constitutes inadequate performance
  - Appropriate sanctions
    - Reduction in fees etc.
Third-Party Service Provider Risks

- Is the vendor/service provider a strategic fit for your organization?
- Is the third-party financially stable?
- Does the system allow for scalability?
- Will you have online access to real-time reports?
- Can velocity limit parameters be established?
- Does the application provide process & system monitoring capabilities?
Information Security

- FI’s should implement the appropriate physical and logical security controls are implemented
- Look at service providers and external networks
- Consider controls on:
  - Origination, approval, transmission and storage of ACH information
  - Corporate Account Takeover
Exposure limits

- Based on the originator’s credit rating
- Relative to all services i.e. (cross-channel)
- Written agreements with Originators addressing exposure
- Separate limit for WEB, IAT
- Increase in unauthorized triggers re-evaluation
ODFI Reports

- Automated for returns (60-75 days)
  - Unauthorized
  - Invalid, other
- Entries in excess of the exposure limit and approval
- WEB monitored separately
- Audits from Originators
Credit Risk

- ODFI Exposure (Credit Entries)
  - Period of time between the initiation of ACH credit file until the company funds the account
  - Amount of risk based on total amount of the file
    - **Up to 2 days**

- ODFI Exposure (Debit Entries)
  - Date funds available to Originator until debits can no longer be returned by RDFI’s
    - Up to 60 days from settlement for unauthorized
    - Can be 2 banking days for NSF/uncollected funds
  - Amount of risk based on amount of individual or multiple returned ACH debits
Balancing procedures
  ✓ General ledger
  ✓ ACH activity with pending file totals
  ✓ Separate accounts for returns, unposted items
Verifies the source of the files originated
Separation of duties
Customer profile change request
ACH Funding

- Adequacy of funding before releasing the file to the Operator
- Prefunding
  - Timing
  - Blocks or separate account
1) Lack of Senior Management & Board Oversight
2) Lack of Adequate MIS and Reporting
3) Lack of Monitoring
4) Inappropriate Approval Process (separation of duties)
5) Inadequate Limits or No Limits
Conclusion

- As electronic payments volume, new products, and entry points continue to increase, financial institutions must have effective and comprehensive policies, procedures, and processes to identify, measure, and limit the risk to the bank and its customers.

- Financial institutions that process payments for third parties including payment processors and high risk merchants must implement enhanced risk management practices to protect against increased credit, compliance/legal, reputational, strategic, and operational risks.
Learning Objectives

- Understand the risks associated with Third-Party relationships
- Understand risk mitigation best practices and requirements