SOUND BUSINESS PRACTICES FOR EVALUATING CUSTOMER RISK

May 2014
SOUND BUSINESS PRACTICES FOR EVALUATING CUSTOMER RISK

Contents

Introduction ................................................. 1
Enterprise-Level Policies, Procedures and Assessments ............ 3
    General Policies, Procedures and Assessments ............ 3
    Regulatory References .................................. 4
    Line of Business-Based Policies ...................... 5
ACH Client Policies, Procedures and Assessments ................. 6
    ACH General Policies, Procedures and Assessments ...... 6
    ACH Line of Business-Based Policies ................. 6
    ACH Activity Policies ................................ 7
    ACH Regulation-Related Policies .................... 8
    ACH Additional Investigation and Recordkeeping ....... 8
ACH Monitoring and Reporting .................................... 9
INTRODUCTION

Sound Business Practices for Evaluating Customer Risks

NACHA – The Electronic Payments Association has developed these sound business practices to aid financial institutions in creating their own internal policies and procedures for appropriate due diligence when assessing and monitoring ACH Originators whose business activities may present a higher than normal risk profile under the institution’s enterprise risk management (ERM) program. Customer risks identified within an ERM program typically include—at a minimum—credit risk, operational risk, regulatory risk and reputational risk. This document also reviews key sound business practices for ACH origination in general.

Under an ERM program, certain industries, geographies or business activities may be identified as presenting higher than normal risk characteristics. As a result, customers that are deemed as potentially presenting a higher risk typically warrant additional due diligence before onboarding and on an ongoing basis to ensure that the financial institution has an appropriate understanding of a customer’s business.

This document details sound business practices that financial institutions may employ, or adapt, to diligently evaluate potential customer risks. The document is divided into two sections: Enterprise-Level Policies and ACH Client Policies. Each section presents a number of practices that financial institutions may want to consider when evaluating customer risk profiles.

Specifically, the two sections address:

**Enterprise-Level Policies, Procedures and Assessments**

- General Policies
- Regulatory References
- Line of Business-Based Policies

**ACH Client Policies, Procedures and Assessments**

- General Policies
- Line of Business-Based Policies
- Activity Policies
- Regulation-Related Policies
- Additional Investigation and Recordkeeping

The sound business practices in this document are not intended to be prescriptive; instead, they provide Originating Depository Financial Institutions (ODFIs) with approaches that may be useful in developing, assessing and tailoring an appropriate and comprehensive due diligence process. Understanding the entire customer relationship helps bring context to the customer’s performance and will assist the institution, at an enterprise level, in assessing the risks of each customer and establishing an appropriate control environment. Cross-departmental communication with other departments such as Compliance (including compliance with the Bank Secrecy Act and Anti-Money Laundering – BSA/AML), Credit and Operations and branch or account managers, is important in any risk strategy.

---

1 In this document, the term “customer” refers to both current and prospective customers.
The sound business practices in this document were developed by NACHA's Risk Management Advisory Group (RMAG), a group established to promote sound business practices for risk management and quality in the ACH network, with contributions from the following individuals:

- Mary Burchette, US Bank
- Nancy Grant, AAP, NCP, NACHA
- Ron Kiefer, City National Bank
- Jerry Meyer, The Bank of Kentucky
- Sara Pinkus, AAP, CAMS, CISA, TD Bank
- Deborah Shaw, AAP, CTP, Federal Reserve Bank of Atlanta

Questions or comments should be directed to NACHA-Ntwrk-Risk@nacha.org.
SOUND BUSINESS PRACTICES FOR EVALUATING CUSTOMER RISK:
ASSESSMENT, ONBOARDING AND REPORTING

Enterprise-Level Policies, Procedures and Assessments

Enterprise-level sound business practices help enable review of a customer’s overall risk profile. In considering the financial institution’s enterprise-level risk exposure to a customer, evaluate all products and services provided to the customer to develop a holistic risk assessment.

A financial institution should consider the following sound business practices when evaluating customer risk.

General Policies, Procedures and Assessments

- Identify and review at the enterprise level, policies covering acceptable customer risk profiles and evaluation of individual customer risk, including, at a minimum:
  - Credit or credit risk policies
  - AML/BSA Policies, which typically include:
    o Industry classification (using, for example, NAICS - North American Industry Classification System)
    o Geographic location
    o Electronic transfer activity
    o Cash activity
  - Legal lending limits and house limits (including ACH exposure limits)
  - Typical categories of customers that use services of specific departments or areas within the financial institution, such as credit services; treasury management; credit cards; remote deposit capture; online services; and merchant services
- Determine if the customer is using, or expects to use, other services and products within the financial institution
  - If so, review the appropriate departmental risk policies and related sound business practices
- Review activities specific to the customer, including, at a minimum:
  - Determine why the customer has come to your financial institution for services. For example, if the customer has changed financial institutions several times in a brief period of time (such as six months), learn the reason(s) for the changes, and consider implications of frequent changes in financial institution relationships for onboarding the customers
  - Identify funds flow – sources and destinations of funds – for all of the customer’s financial institution activity
    o Determine internal processes for reporting customer problems, fraud and potential fraud. That is, identify the actions that take place internally when problems with an origination customer arise (or are believed to have arisen). Determine whether there have been issues with the customer within other areas of the
**SOUND BUSINESS PRACTICES FOR EVALUATING CUSTOMER RISK:**

**ASSESSMENT, ONBOARDING AND REPORTING**

- financial institution or with another financial institution.
  - Ask the customer about any issues with other financial institutions, i.e. what they were, and how they were resolved
  - Determine risk criteria for terminating a customer relationship

<table>
<thead>
<tr>
<th>Regulatory References</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Consider regulatory guidance when defining customer categories, including but not limited to the following:</td>
</tr>
</tbody>
</table>
|   - FFIEC – Supplement to Authentication in an Internet Banking Environment, issued June 28, 2011  
|   - FinCEN – Risk Associated with Third-Party Payment Processors, issued October 22, 2012  

- Be familiar with and stay up to date with changes in applicable state regulations, using the same or similar methods as are used to stay up to date with state regulations for other areas in the financial institution
- Continuously monitor the regulatory environment for identification of lines of business that are deemed as possibly posing an elevated level of risk
**SOUND BUSINESS PRACTICES FOR EVALUATING CUSTOMER RISK:**

**ASSESSMENT, ONBOARDING AND REPORTING**

| Line of Business-Based Policies | • Determine whether a potential client is active in lines of business that are associated with unfair, deceptive or abusive marketing and sales tactics  
• Identify lines of business in which your financial institution has little or no interest or that are not in your financial institution’s business model. Common examples include gaming, adult entertainment, and debt relief. Clarify whether businesses that operate one or more of these lines of businesses are categorically unacceptable or whether additional assessments and reviews are required before accepting on such businesses as financial institution customers.  
• When carrying out enhanced due diligence, consider requesting from the customer:  
  – Tax returns  
  – Financial statements  
  – Customer lists  
  – Sample contracts  
  – Due diligence procedures for downstream customers  
  – Identification of beneficial owner(s) of the business |

---

Page 5 of 10
**SOUND BUSINESS PRACTICES FOR EVALUATING CUSTOMER RISK:**

**ASSESSMENT, ONBOARDING AND REPORTING**

**ACH Client Policies, Procedures and Assessments**

ACH client-related sound business practices provide a framework for assessing potential customer risk around ACH services. A financial institution should consider the following sound business practices when evaluating ACH-specific customer risk. ODFIs that originate ACH entries on behalf of their customers should be aware that both they and their Originator and Third-Party customers are subject to the *NACHA Operating Rules* and applicable U.S. law.

| ACH General Policies, Procedures and Assessments | • Review requirements for ACH customers, including but not limited to:  
| | ‒ Prefunding  
| | ‒ Requiring the customer to also be a borrower  
| | ‒ Requiring deposits over a certain threshold  
| | ‒ Requiring collateral  
| | ‒ Risk-based pricing  
| | • Identify policies, procedures and assessments that are in place for assessing ACH customer risk in addition to those that are in place for routine customer assessment  
| | • Determine if the customer uses multiple financial institutions for ACH services  
| | ‒ If the customer uses multiple financial institutions, determine which financial institutions they use for which services  
| | ‒ Understand the customer’s business reason for using multiple financial institutions and how they select primary and secondary financial institutions  
| | • Determine the nature of other relationships the Originator has within the financial institution (deposit, lending, services, etc.)  
| | • Document results of investigation of a customer and steps taken to obtain and assess information around customers that may pose a higher level of risk, as well as any relationships with Originators and Third-Parties.  
| ACH Line of Business-Based Policies | • Identify classifications of businesses and transactions that are of specific concern to ACH:  
| | ‒ Identify concerns for business types defined as more likely to pose an elevated level of risk and determine what actions should be taken to address those concerns  
| | ‒ Understand the products or services that the Originator is selling and its target audience  
| | ‒ Ensure that authorizations for such products or services comply with *NACHA Operating Rules*  

Page 6 of 10
**SOUND BUSINESS PRACTICES FOR EVALUATING CUSTOMER RISK:**

**ASSESSMENT, ONBOARDING AND REPORTING**

<table>
<thead>
<tr>
<th>ACH Activity Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Review potential exposure limits to determine if they will typically exceed a certain threshold. Exposure limits should take into account the overall financial worth of the customer over multiple settlement days.</td>
</tr>
<tr>
<td>• If potential daily or multi-day exposure is in excess of a financial institution threshold or involves other extensions of credit in addition to those associated with ACH activity, complete a more in-depth financial analysis and gain all necessary approvals for accepting higher exposure.</td>
</tr>
<tr>
<td>• Review historical return rates (if data is available) and expectations for ongoing return rates:</td>
</tr>
<tr>
<td>• Examine return rates, and in particular return rates for unauthorized transactions</td>
</tr>
<tr>
<td>• Take appropriate mitigating actions when return rates, especially rates for NSF (insufficient funds), invalid or unauthorized returns, increase or are out of pattern.</td>
</tr>
<tr>
<td>• Ensure compliance with the ODFI Return Requirements Rule, which requires that the return rate for unauthorized transactions be held under 1 percent.</td>
</tr>
<tr>
<td>• Determine and review with the Originator the reasons for increased or out-of-pattern returns and require additional steps to lower return rates for all Return Reason Codes</td>
</tr>
<tr>
<td>• Review requests from RDFIs and others for proof of authorization, as such requests – particularly an increase in the number of requests – are often an early sign of potential problems</td>
</tr>
<tr>
<td>• Determine what additional reporting requirements are currently required for ACH customers that pose, or may pose, a higher than typical level of risk, and what additional requirements may be applicable for a given customer</td>
</tr>
<tr>
<td>• Produce appropriate reports for Line or Senior Management, Risk Committees, Anti-Money Laundering (AML) staff, and the Board of Directors, including the ability to:</td>
</tr>
<tr>
<td>o List, on demand, ACH customers that pose, or may pose, an elevated level of risk</td>
</tr>
<tr>
<td>o Report on activities of customers that pose, or that may pose, an elevated level of risk</td>
</tr>
<tr>
<td>o List Third-Parties with which the financial institution has relationships</td>
</tr>
</tbody>
</table>
# Sound Business Practices for Evaluating Customer Risk:
## Assessment, Onboarding and Reporting

- Report on activities of Third-Parties with which the financial institution has relationships
  - Determine appropriate frequency of monitoring/review of activity. High-volume Originators and Originators in businesses representing elevated risks may warrant more frequent monitoring for anomalous behavior
  - Ensure that review procedures are in place to escalate unusual activities (for example, a payroll company that has historically originated few debits – because most of its transactions were credits to employee accounts, tax authorities and the like – begins to originate large numbers of debits)

### ACH Regulation-Related Policies
- Perform due diligence around regulatory, business and consumer issues:
  - Visit the FTC website (ftc.gov) to search for consumer complaints on a specific company or to search for any negative information about principals of prospective customers
  - Contact, or visit the website of, the appropriate (by geography) Better Business Bureau for the customer’s grade and to determine whether complaints have been filed against the business
  - Perform reviews of the business and principals utilizing independent third-party databases to validate information about the business and its principals
  - Identify any judgments against or negative news related to the company and/or its principals
  - In some cases, consider whether it is appropriate to check consumer complaint websites, such as that provided by the CFPB at consumerfinance.gov, ripoffreport.com, and complaints.com.

### ACH Additional Investigation and Recordkeeping
- Check the Originator Watch List database to see if a customer is listed to determine whether additional due diligence is necessary to evaluate customer risk.
- Check the Terminated Originator Database to determine if a customer has been terminated from another financial institution
- If you do not participate in the Terminated Originator Database, consider doing so (https://www.nacha.org/Terminated_Orginator_Database)
- For Third-Parties, such as Third-Party Service Providers and Third-Party Senders:
  - Refer to NACHA publications Third-Party Senders and the ACH Network and Identifying Third-Party Business Models: Common Business Models & Sound Business Practices
  - Determine and track downstream organizations and review/assess each as if it were to be a direct Originator
  - Record decision-making around a potential customer
  - If the customer is accepted for ACH origination, record the reasons and retain supporting documentation
SOUND BUSINESS PRACTICES FOR EVALUATING CUSTOMER RISK:
ASSESSMENT, ONBOARDING AND REPORTING

ACH Monitoring and Reporting

- Monitor activity day-to-day and across multiple settlement dates to establish regular patterns of origination and returns, both in volume and dollars
- Investigate out-of-pattern activity promptly and, if issues are identified, move quickly to resolve them
- Monitor and examine ACH activity periodically for consistency with type of business, especially for high-volume Originators.
  - Consider establishing activity thresholds beyond which additional reviews may be necessary, such as:
    - Rapid increases in number of transactions and/or dollar volume
    - Changes in the debit/credit mix
    - Increases – even small – in the number and/or percent of returns overall, and in particular, unauthorized and invalid returns
    - Track number of requests for proof of authorization for originated transactions
- Communicate and collaborate with other internal departments and the branch/account manager to understand the nature of the customer’s ACH activity
- Determine internal processes for reporting customer problems, fraud, potential fraud; that is, what happens internally when problems with an origination customer arise
- Determine internal processes for remediating unacceptable activities, and/or enforce restrictions on the types of ACH transactions that may be originated in accordance with the Origination Agreement
  - This may include consulting with the customer to change business practices that lead to elevated levels of risk
  - If activity persists, consider revoking ACH origination services and/or exiting the relationship
- Record decision-making around decisions to terminate a current customer or to deny a customer additional services, lines of credit, etc.
  - Be specific in the reasons, including relevant data or specific activities
  - Record individuals and departments involved in the decision
  - Enter information about the terminated customer into the Terminated Originator Database (if you participate in the service)
    - If you do not participate in the Terminated Originator Database, consider doing so
SOUND BUSINESS PRACTICES FOR EVALUATING CUSTOMER RISK:

ASSESSMENT, ONBOARDING AND REPORTING

(https://www.nacha.org/Terminated_Originator_Database)

These sound business practices will help support financial institution evaluations of customer risk. For education support on how to implement these sound business practices, visit: https://www.nacha.org/Education

Or contact your Regional Payments Association. Questions or comments on the sound business practices should be directed to: NACHA-Ntwrk-Risk@nacha.org

# # #