The I Do's and I Don'ts of Third-Party Sender Relationships

Presented by:

Macha/PAR – Everything Payments - Everywhere

Jessica Lelii, AAP, APRP, NCP

Director of Education

www.macha.org

jlelii@macha.org

DISCLAIMER

Macha, through its Direct Membership in Nacha, is a specially recognized and licensed provider of ACH education, publications and support.

Payments Associations are directly engaged in the Nacha rulemaking process and Accredited ACH Professional (AAP) program.

Nacha owns the copyright for the Nacha Operating Rules & Guidelines.

The Accredited ACH Professional (AAP) and Accredited Payments Risk Professional (APRP) is a service mark of Nacha.

This material is derived from collaborative work product developed by Nacha and its member Payments Associations and is not intended to provide any warranties or legal advice and is intended for educational purposes only.

This material is not intended to provide any warranties or legal advice and is intended for educational purposes only.

This document could include technical inaccuracies or typographical errors and individual users are responsible for verifying any information contained herein.

© 2024 Macha/PAR All rights reserved

Agenda

- TPSP vs. TPS
- TPS Policy
- Due Diligence
- Agreements
- Ongoing Monitoring
- Risk Management

TPSP vs. TPS

Third-Party Service Provider

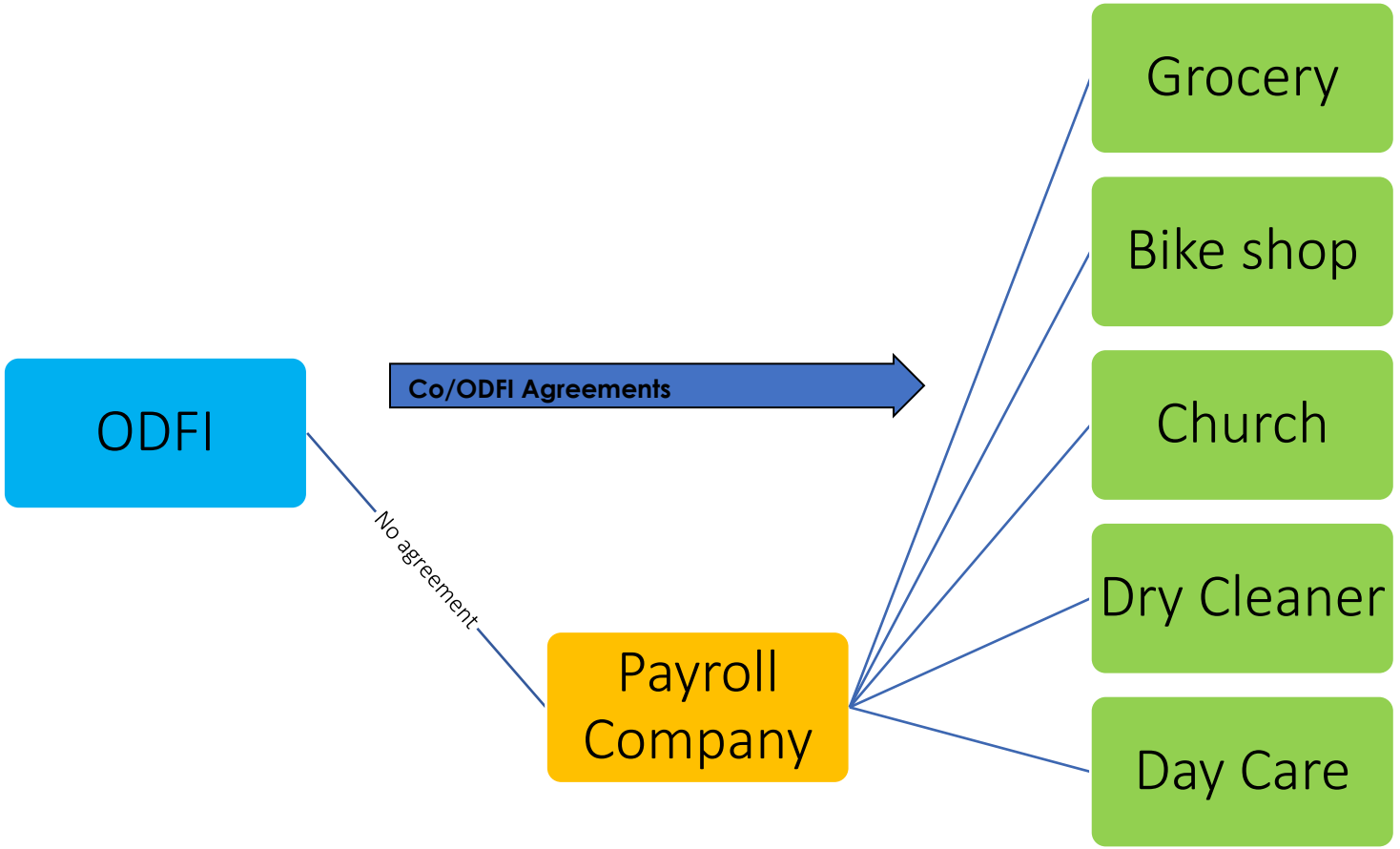
an Organization that performs any functions on behalf of the Originator, the Third-Party Sender, the ODFI, or the RDFI (not including the Originator, ODFI, or RDFI acting in such capacity for such Entries) related to the processing of Entries, including the creation of the Files or acting as a Sending Point or Receiving Point on behalf of a Participating DFI. An Organization acting as Third-Party Sender also is a Third-Party Service Provider.

Third-Party Sender

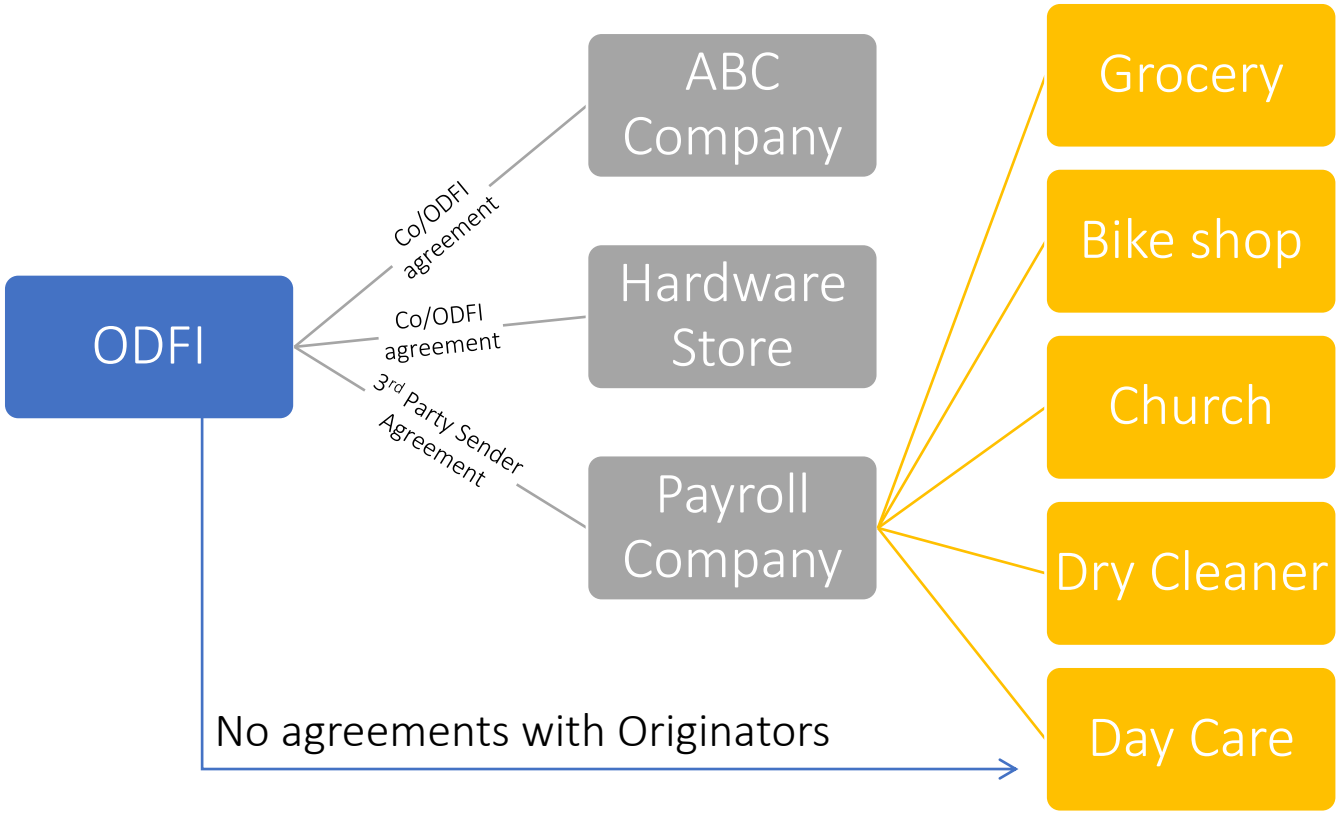
a type of Third-Party Service Provider that acts as an intermediary on behalf of an Originator or another Third-Party Sender in Transmitting Entries between the Originator and the ODFI, when there is not an Origination Agreement directly between the Originator and ODFI. A Third-Party Sender must have an Origination Agreement with an ODFI or with another Third-Party Sender.

A Third-Party Sender is never the Originator for Entries it Transmits on behalf of another Organization; however, a Third-Party Sender of Entries may also be an Originator of other Entries in its own right.

Third-Party Service Provider

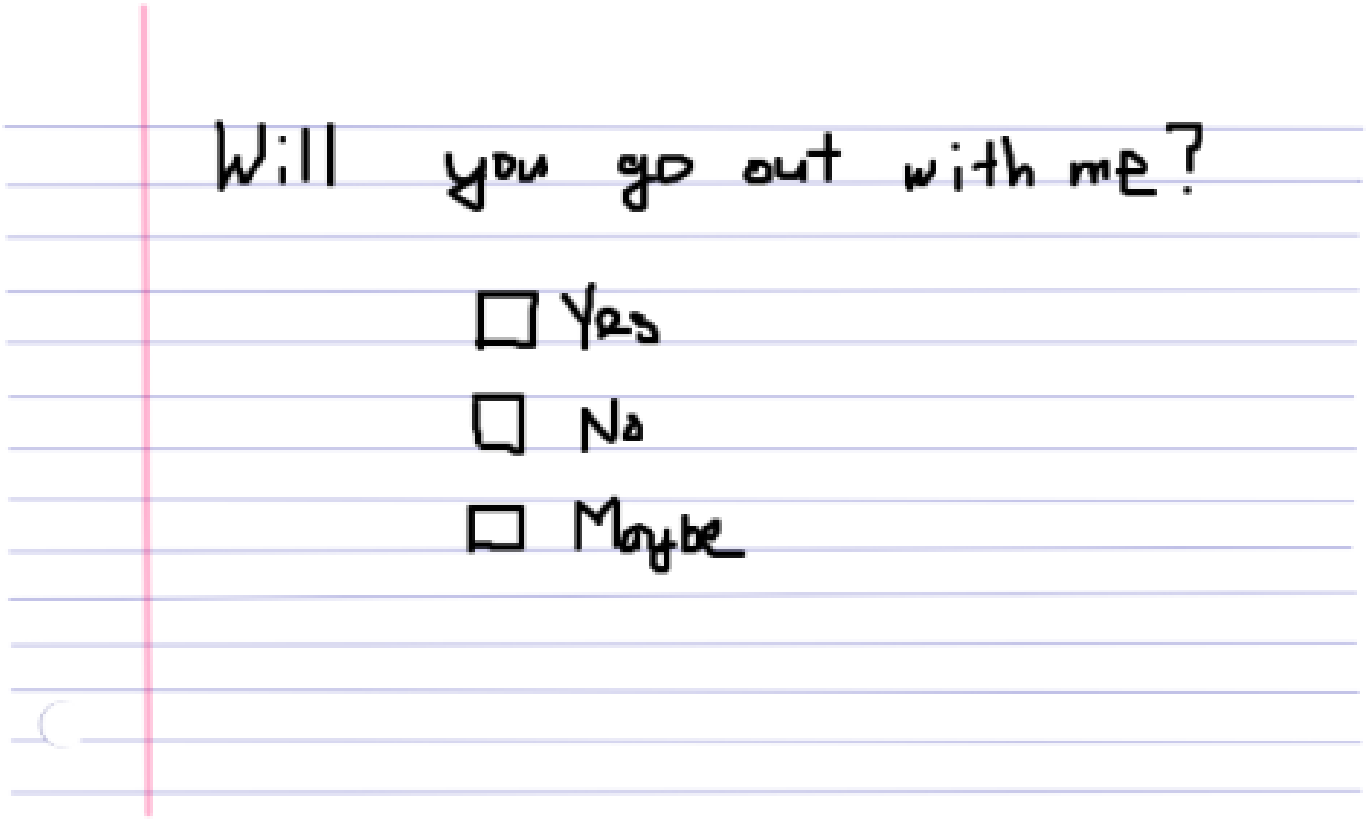


Third Party Sender



Third-Party Sender Policy

- Will you, or won't you?
- Acceptable types of Third-Party Senders
- Acceptable types of downstream Originators
- Nested Third-Party Senders?
- Due diligence
- Risk rating
- Underwriting/exposure limits
- Settlement
- Broad compliance requirements
- Risk management framework



Nice to meet you…will you go out with me?

Due Diligence

- ODFI must utilize a commercially reasonable method to verify the identity of an Originator or Third-Party Sender
- Verify legal existence and financial standing
  - Company financials
  - Payment history
  - Company principles and Beneficial ownership
  - Credit bureaus, BBB, D&B, etc.
- Assess inherent risks
  - Nature of activity
  - List of Originators
    - Nature of the businesses being processed for
  - Payment velocity
  - Normal Dollar value of files
  - Return and other exception statistics
  - Written policy on onboarding and terminating Originators

Due Diligence

- Gather relevant information
  - Personalize questionnaires and data collection to only include pertinent questions and solicit essential documents based on identified concerns
- Analyze incoming information and validate prospects
  - Subject matter experts should be available to review and evaluate risk factors and opportunities in areas such as
    - IT security
    - Data privacy
    - Financial stability

Will you marry me? (but I need a prenup)

Third-Party Sender Agreements

An ODFI must enter into an Origination Agreement with each Third-Party Sender. The agreement must contain, at a minimum:

- The Third-Party Sender, on behalf of the Originator, must authorize the ODFI to originate Entries on behalf of the Originator to Receivers' accounts
- The Third-Party Sender must agree to be bound by the Rules
- The Third-Party Sender must agree not to originate Entries that violate the US laws
- Any restrictions on the types of Entries that may be originated
- The right of the ODFI to terminate or suspend the agreement, or any Originator or Nested Third-Party Sender of the Third-Party Sender, for breach of the Rules in a manner that permits the ODFI to comply with the Rules
- The right of the ODFI to audit the compliance with the Origination Agreement and the Rules by the Third-Party Sender, any Nested Third-Party Senders, and their respective Originators
- Any restrictions on Nested Third-Party Senders
- The Third-Party Sender must agree that, before permitting an Originator to originate any Entry directly or indirectly through itself or the ODFI, it will enter into an agreement with the Originator that satisfies the requirements of the Rules
- The Third-Party Sender must agree that, before permitting a Nested Third-Party Sender to originate any Entry directly or indirectly through itself or the ODFI, it will enter into an agreement with the Nested Third-Party Sender that satisfies each of the requirements of the Rules and must agree to be responsible for the Nested Third-Party Sender's compliance with these Rules

Third-Party Sender Agreements-Other Considerations

- Restricted Originators
- Compliance
- Security procedures
- Allocation and assumption of risk and loss
    - Liability for errors
    - Fraud
- Risk assessment
- Business continuity management and disaster recovery (BCM/DR)

Third-Party Sender Agreements-Other Considerations

- Data breach or compromise
- OFAC
- Exposure limits
    - Underwriting standards or procedures
- Cancelation, amendment or rejection of entries
    - Right to reject entries
    - Timeframe for notification of rejected entries
    - Timeframe for remaking files or entries
- Delays in processing
- Same-Day ACH

Third-Party Sender Agreements-Other Considerations

- Account verification requirements
  - Prenotifications
  - Micro-Entries
- SEC code requirements
- Originator's obligation to obtain valid authorizations
  - Proper authorization methods, forms and formats
  - Must provide to ODFI upon request
- Record retention
  - ACH data
  - Authorizations
- Settlement/Account requirements
  - Prefunding
  - Funding method, required balances, collateral, NSF

Third-Party Sender Agreements-Other Considerations

- Error detection/notification
- Reversals
  - Timeframes
  - Permissible reasons
- Notice of returns and NOCs
  - Administrative returns < 3%
  - Overall returns < 15%
- Retry Payments
- Return Fee entries
- Unauthorized entries
  - Unauthorized return rate < 0.5%
- Fees
- Rules Enforcement

This marriage thing is great!

What’s next?

- TPS must periodically, or upon request, provide the ODFI with information on their Originators
- ODFI must establish, implement, and periodically review an exposure limit for the Third-Party Sender
- ODFI must establish procedures to:
- Monitor the Originator’s or Third-Party Sender’s origination and return activity across multiple Settlement Dates
- Enforce restrictions on the types of Entries that may be originated
- Enforce exposure limits

Risk Assessment

- Third-party Senders must conduct a risk assessment of the risks of their activity
- Risk assessment should:
  - Estimate the significance of the risk
  - Assess the likelihood or frequency of the risk occurring
  - Consider how the risk should be managed and assess what action must be taken
- No prescribed methodology regarding-
  - Frequency
  - Content
  - Who conducts the risk assessment
  - How to rate or evaluate risk
- Guidance available from Regulators or FFIEC

FFIEC Guidance on Risk Assessment

- Risk assessment is the process of identifying risks to operations, organizational assets, individuals, and other organizations
- Incorporates threat and vulnerability analyses and addresses the appropriate mitigations
- Risk assessment should be commensurate with the entity's risk and complexity
- Includes:
  - Risk Identification
  - Risk Analysis

FFIEC IT Examination Handbook, Business Continuity Management

Risk Management

- Annual Rules compliance audit
- ACH Origination Agreements
- Exposure Limits
- KYC and KYCC
- Physical access controls
- Privilege based user access controls
- Multi-factor authentication
- Out of band verification
- Physical security
- BCP Plans – develop and test disaster recovery plans

Questions

AAP™
Accredited
ACH Professional

APRP™
Accredited Payments
Risk Professional

Continuing Education Credits

The I Do's and I Don'ts of Third-Party Sender Relationships

August 2024

This session is worth 1.8 credits

(keep this slide for your records)