CSBS SINCE 1902

CONFERENCE OF STATE BANK SUPERVISORS

Third Party Payment Processors Job Aid

This job aid is to be used by state institution examiners as a means to understand, identify, and assess the risks associated with institutions' relationships with a common type of third-party service provider, third-party payment processors or senders, herein referred to as TPPPs or processor(s). This job aid was developed through the State Examiner Review Team in response to findings from the 2013 CSBS Examiners Forum and the CSBS Risk Identification Team. This job aid is not intended to guide a review of an institution's broader vendor management program.

Smaller community institutions are particularly susceptible to TPPP abuse, as they may lack the infrastructure and expertise to properly manage and monitor these relationships. With this in mind, this job aid provides:

- Examples of how financial institutions and their processor customers send transactions through the Automated Clearing House (ACH) network.
- A better understanding of how an institution's risk profile may change by assuming a processor as a customer.
- Examination procedures to ensure the institution is adequately monitoring, reviewing, and verifying depository relationships with a processor.

Contents

BACKGROUND

Third Party Payment Processors (TPPPs or processor(s)) originate transactions for consumers or businesses that are not direct customers of the originating financial institution. They provide payment processing services to merchant or business clients, and group these payments together to take advantage of economies of scale. They are one type of third party service providers (TPSPs), which is a broad category of third party relationships. Processors use their deposit accounts to conduct payment processing on behalf of their different clients. Financial institutions can earn attractive fee income by facilitating these transactions, and this has led to an increasing number of institutions entering into depository relationships with processors.

TPPPs most frequently offer their clients payment services via the Automated Clearing House (ACH) network, and "some of the most problematic activity occurs in the origination of ACH debits or the creation and deposit of remotely created checks."[1]

Financial institutions that allow processors to establish deposit relationships for the purposes of processing transactions may find that these relationships expose them to a greater level of compliance, credit, and legal risk. The heightened risk exposure often results from the riskiness of a processor's underlying clients. Processors may deliver services to clients that engage in deceptive, abusive, or illegal practices, and institutions providing depository services to payment processors may be viewed as facilitating such practices. Therefore, institutions and examiners must be aware of these risks, and should be able to identify potential problems by understanding where these risks are most likely to appear. Insufficiently managing such risks could result in enforcement and legal actions. The FDIC has advised institutions that:

> *Financial institutions that fail to adequately manage these relationships may be viewed as facilitating a payment processor's or merchant client's fraudulent or unlawful activity and, thus, may be liable for such acts or practices.*[2]

[1] "Third-Party Payment Processor Relationships." *Supervisory Insights*, Volume 8, Issue 1, Summer 2011, p. 4.
[2] "Payment Processor Relationships: Revised Guidance (FIL-3-2012)." Federal Deposit Insurance Corporation, January 31, 2012, p. 2.

DEFINITIONS

To understand these relationships, it is helpful to understand common arrangements and key terms. In general, an ACH transaction is a batch-processed, value-dated, electronic funds transfer between an originating and a receiving institution. Third-party service providers, which include processors and senders, aggregate and process batches of ACH transactions for clients in order to take advantage of economies of scale.[3] Within the ACH system, these participants and users are known by the following terms:

- ***Originator*** An organization or person that initiates an ACH transaction to an account either as a debit or credit.

- ***Originating Depository Financial Institution (ODFI)*** The Originator's depository financial institution that forwards the ACH transaction into the national ACH network through an ACH Operator.

- ***ACH Operator*** An ACH Operator processes all ACH transactions that flow between different depository financial institutions. An ACH Operator serves as a central clearing facility that receives entries from the ODFIs and distributes the entries to the appropriate Receiving Depository Financial Institution. There are currently two ACH Operators: FedACH and Electronic Payments Network (EPN).

- ***Receiving Depository Financial Institution (RDFI)*** The Receiver's depository institution that receives the ACH transaction from the ACH Operators and credits or debits funds from their receivers' accounts.

- ***Receiver*** An organization or person that authorizes the Originator to initiate an ACH transaction, either as a debit or credit to an account.

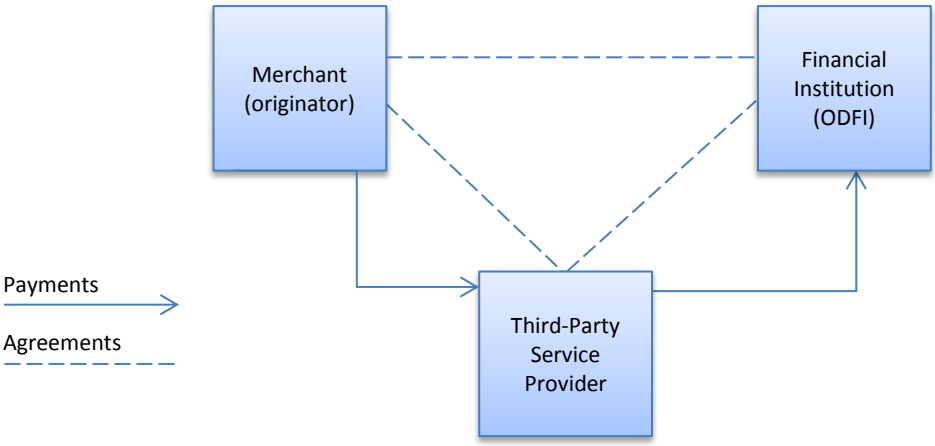
- ***Gateway*** A financial institution, ACH Operator, or ODFI that acts as an entry or exit point to or from the US ACH network. A formal declaration of status as a Gateway is not required. ACH operators and ODFIs acting in the role of Gateway Operators have specific warranties and obligations related to certain international entries. A financial institution acting as a Gateway generally may process inbound and outbound debit and credit transactions. ACH Operators acting as a Gateway process outbound debit and credit entries, but can limit inbound entries to only credit entries and reversals.

- ***Third-Party Service Provider*** An entity other than an Originator, ODFI or RDFI that has an agreement to perform any function on behalf of an Originator, ODFI, or RDFI with respect to the processing of ACH entries. See figure 1.

- ***Third-Party Sender*** A type of third party service provider that acts on behalf of the originator only. See figure 2.

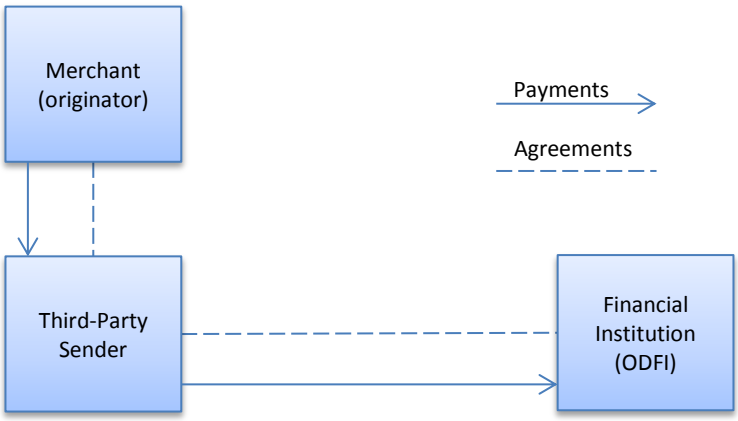
[3] FFIEC BSA/AML Examination Manual, Automated Clearing House Transaction – Overview, 2010, page 225

Figure 1. A common third-party service provider relationship



In Figure 1, the merchant's transactions are batched and processed by the third party service provider, possibly a processor.

Figure 2. A common third-party sender relationship



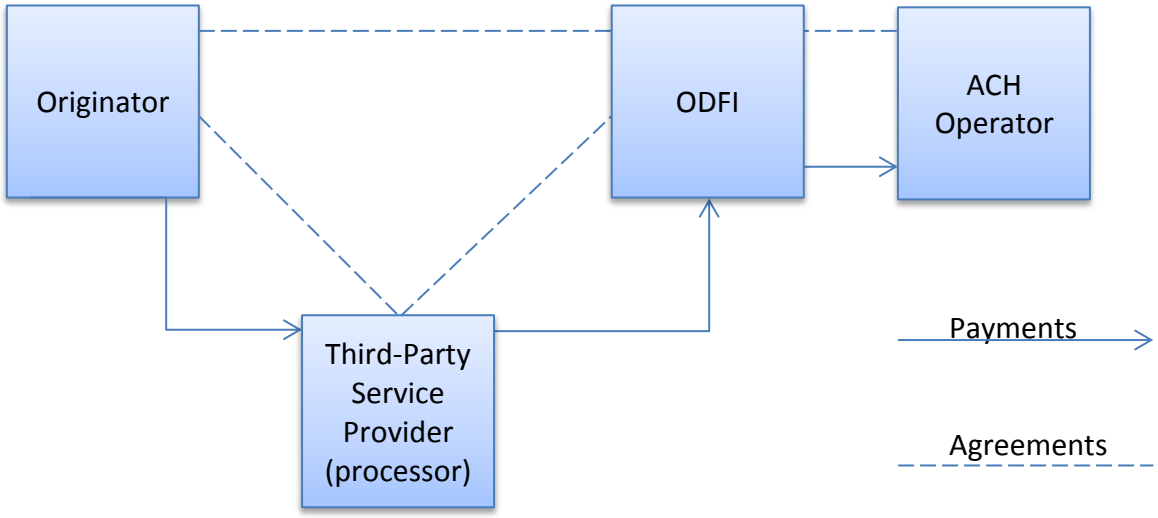
A third party sender is a type of third party service provider that acts on behalf of the originator only. In other words, it is an intermediary between the originator and the ODFI. In this type of relationship, there is generally no contractual agreement between the ODFI and the originator.

A 2006 bulletin[4] by the Office of the Comptroller of the Currency discusses additional relationship structures and more fully explains various ACH activities.

[4] "Automated Clearing House Activities." Office of the Comptroller of the Currency, September 1, 2006. http://www.occ.gov/news-issuances/bulletins/2006/bulletin-2006-39.html

COMMON PROCESSOR/FINANCIAL INSTITUTION RELATIONSHIPS

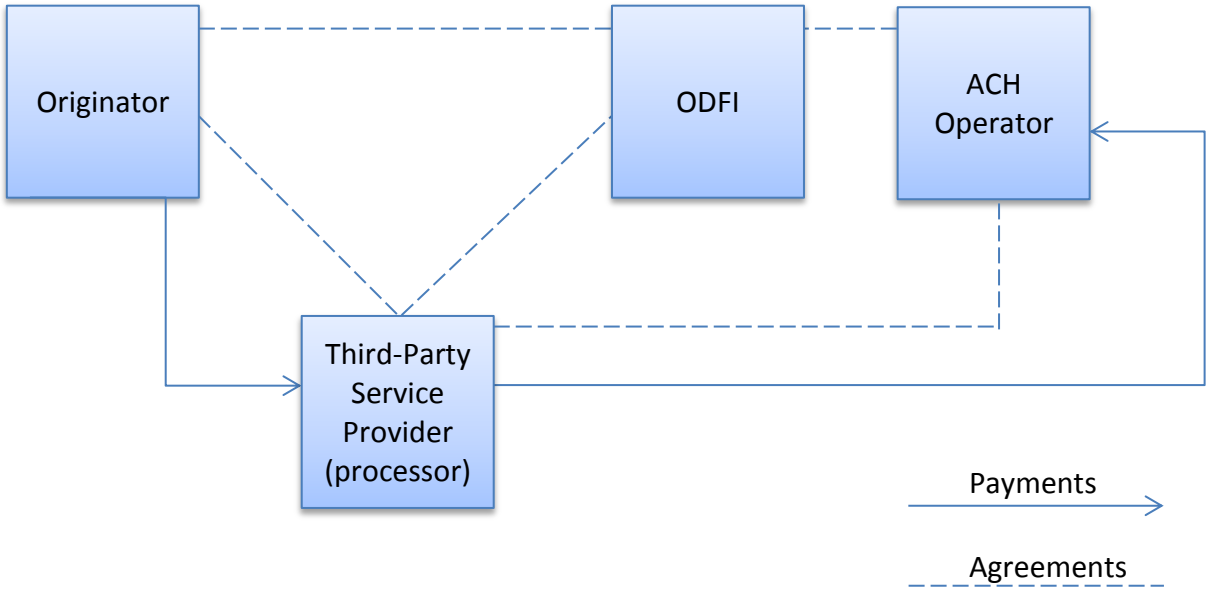
Figure 3. The flow of funds of a Third-Party Service Provider[5]



The use of third parties, including payment processors, in ACH transactions adds complexity and increases an institution's exposure to compliance, credit, transaction, and reputation risks. In cases where a processor conducts activities on behalf of an institution, the institution remains legally responsible for transaction activity, despite the fact that it may not have direct control over the functions performed by the third party.

[5] "Automated Clearing House Activities." Office of the Comptroller of the Currency, September 1, 2006.

Figure 4. The flow of funds of a Third-Party Service provider with direct access to the ACH operator[6]



A third-party service provider may transmit ACH transactions directly to an ACH Operator using the institution's routing number, provided it has obtained permission from the institution. However, the institution warrants the validity of each entry transmitted by the service provider, including the basic requirement that a receiver has authorized each entry.[7] An institution that permits an originator or a third party (either its third-party service provider or an originator's third-party sender) to have direct access to the ACH Operator should maintain control over its own settlement accounts at all times. To do so, an institution should enter into a written contract with the party granted access outlining the rights and responsibilities of the parties, and include a provision permitting the institution to audit the party granted access, as needed, to monitor performance and ensure compliance with applicable laws and regulations. More information on rights and responsibilities of institutions and processors can be found in the *Examination Workprogram.*

Direct Access is an arrangement in which an Originator, Third-Party Sender or a Third-Party Service Provider transmits credit or debit entries directly to an ACH Operator using an ODFI's routing number and settlement account.

Entities that have direct access capability must be sponsored by an ODFI, must have a contract in place, and must be registered as a Direct Access Participant. The Direct Access Registration Rule requires all ODFIs to register their Direct Access Debit status with NACHA.

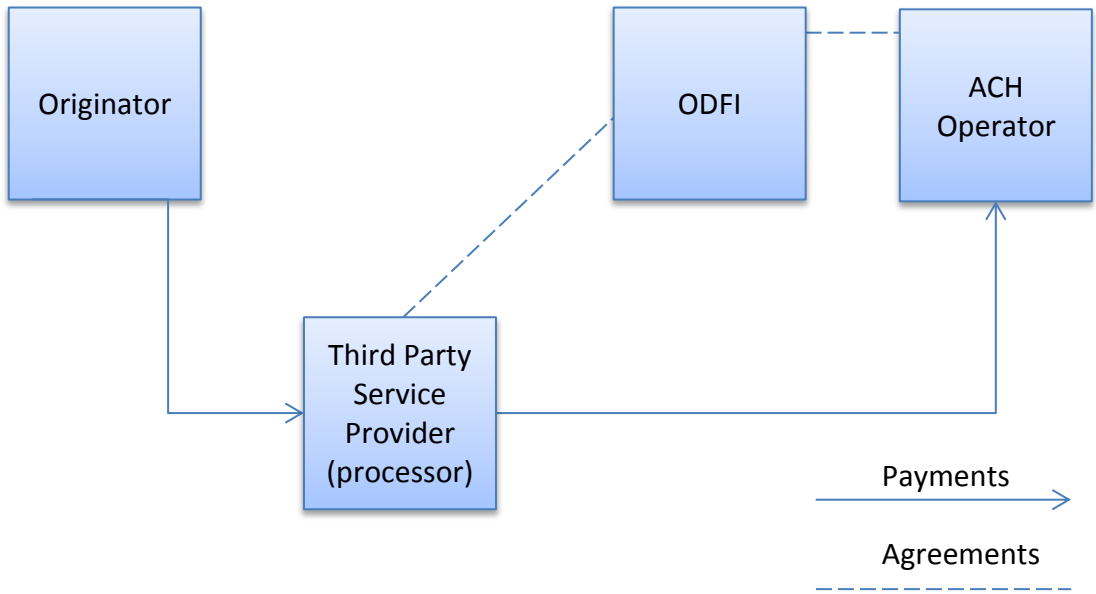
[6] "Automated Clearing House Activities." Office of the Comptroller of the Currency, September 1, 2006
[7] Ibid.

A Direct Access Debit Participant is an Originator, Third Party Sender, or a Third Party Service provider with direct access for the origination of debit entries with the exception of; 1) a TPSP that transmits ACH files solely on behalf of an ODFI where that TPSP does not have a direct agreement with an Originator (and is not itself an Originator, or 2) an ODFI that transmits files using another participating financial institution's routing number and settlement account. [8]

As part of the Direct Access Registration Rule, an ODFI must complete their registration by either: 1) acknowledging a statement to the effect that they have no direct access debit participants or 2) providing specific information about each Direct Access Debit Participant.

[8] Direct Access Registration. NACHA. (https://www.nacha.org/directaccessreg)

Figure 5. The flow of funds of a Third-Party Service Provider with direct access and no originator-processor agreement



Occasionally, third-party processors/senders process transactions for originators that may not be governed by an agreement. Such arrangements expose the ODFI to substantial risk and limit the ability of the ODFI to perform the necessary due diligence.

RISK EXPOSURES

Before establishing any banking relationship with a processor, institution management should consider how the relationship will alter their risk profile. This is best done through the risk assessment process. These relationships have the potential to change the institution's risk profile from the standpoints of liquidity, fraud, BSA/AML, consumer protection, legal liability, and overall safety and soundness.

- ***Liquidity risk*** Processors may require the transmission of a large dollar volume from their deposit account. Institutions should monitor the average volume and remain prepared to deal with large outflows or inflows of cash.

- ***Fraud risk*** Increasingly, instances of merchant fraud are being detected through institutions' relationships with processors. Fraud can take many forms, from unauthorized transactions using stolen account numbers to repeated debit entries by an illegal merchant. Additionally, "the risk of fraud arises when an illicit telemarketer or online merchant obtains the consumer's account information through coercion or deception and initiates an ACH debit transfer that may not be fully understood or authorized by the customer."[9]

- ***Compliance, BSA/AML risk*** ACH transactions that are originated through a TPPP may increase compliance risks, making it difficult for an ODFI to underwrite and review Originator transactions for compliance with state and federal regulations. Risks are heightened when neither the TPPP nor the ODFI performs due diligence on the companies or individuals for whom they are originating payments. Certain ACH transactions, such as those originated through the Internet or by telephone, may be susceptible to manipulation and fraudulent use. Certain practices associated with how the banking industry processes ACH transactions may expose institutions to compliance risks. These practices include:
    - An ODFI authorizing a TPPP to send ACH files directly to an ACH Operator, in essence bypassing the ODFI.
    - ODFIs and RDFIs relying on each other to perform adequate due diligence on their customers.
    - Batch processing that obscures the identities of originators.
    - Inadequate information sharing practices regarding originators and receivers that inhibit an institution's ability to appropriately assess and manage the risks associated with correspondent and ACH processing operations, monitor for suspicious activity, and screen for OFAC compliance.

[9] "Third-Party Payment Processor Relationships." *Supervisory Insights*, Volume 8, Issue 1, Summer 2011, p. 4.

- ***Consumer protection and liability risk*** High-risk or illegal merchants may attempt to process transactions through a processor. These transactions may be considered unfair or deceptive, as defined by the Federal Trade Commission Act. As previously mentioned, "Financial institutions that fail to adequately manage these relationships may be viewed as facilitating a payment processor's or merchant client's fraudulent or unlawful activity and, thus, be liable for such acts or practices."[10] In other words, if processing an illegal transaction results in harm to a consumer, the institution may be required to pay restitution and/or civil money penalties.

- ***Reputational risk*** In some cases, processors target small, community institutions because of their perceived lack of control and ongoing monitoring. In these cases, the reputational risks are heightened. For example, news of a large loss sustained from a failed processor relationship may impact the community's perception of the safety and soundness of an institution.

- ***Credit risk*** Processors' deposit accounts can become overdrawn quickly, often due to returns and chargebacks. A troubled processor's debt may become uncollectible, presenting credit risk to the institution.

[10] "Payment Processor Relationships…" Op. cit., p. 2.

REFERENCES

FDIC Financial Institution Letters:

- FIL-43-2013: Supervisory Approach to Payment Processing Relationships with Merchant Customers that Engage in Higher-Risk Activities
- FIL-3-2012: Payment Processor Relationships (revised guidance)
- FIL-44-2008: Guidance for Managing Third Party Risk
- FIL-127-2008: Guidance on Payment Processor Relationships (supplemented by FIL-3-2012)

ED Module: Third Party Risk

OCC guidance 12-2008: Payment Processors

OCC Bulletin 29-2013: Third-Party Relationships

OCC Bulletin 39-2006: Automated Clearing House Activities

FFIEC BSA/AML InfoBase: *Third-Party Payment Processors--Overview*

FDIC Supervisory Insights Article (Summer 2011): Managing Risks in Third Party Payment Processor Relationships (pages 3-12)

FinCEN Advisory Fin 2012-A010, Risk Associated with Third Party Payment Processors

NACHA Originator Watch List (OWL)

EXAMINATION WORKPROGRAM

The following workprogram is based largely on FDIC Financial Institution Letter (FIL) 3-2012. Except for section A, the workprogram is designed so that areas of potential risk will be answered with "no." Affirmative answers indicate the institution is taking the proper risk control steps.

If adverse findings are discovered, the examiner should discuss the findings with the Examiner-in-Charge and institution management. Further analysis, such as transaction testing, may be necessary. Depending on the severity, deficiencies may be cited in the report of exam and may warrant a downgrade of the "Management" or "Information Technology" rating. *Examiner Notes* explain a concept or provide action steps.

The following documents may be helpful to obtain before beginning this workprogram:

1. Applicable policy or operating procedures
2. Documentation on existing third-party relationships
3. Agreements between institution and any processor
4. Risk assessments
5. Report of chargeback and return activity for each processor
6. Correspondence from NACHA, which may include:
    a. A *Notice of Possible ACH Rules Violation*
    b. *Notice of Possible Fine*

	UNDERSTANDING PRESENT ACTIVITIES *Examiner note: This section should be completed to develop an understanding of the institution's activity level and potential risk exposure. If any of the answers are "Yes," a potentially high-risk customer or relationship may be present. The examiner is then encouraged to focus on Section C, Management Practices & Controls.*	**Y**	**N**	**Examiner Comments** [Document supporting evidence and note determinations and findings made.]
A.1	Does the institution provide ACH services as an/a: • Originating Depository Financial Institution (ODFI)? • Receiving Depository Financial Institution? *Examiner note: If the institution is not an ODFI, then the risk of exposure to TPPP risk is very limited and the remaining steps may not be necessary.*			
A.2	Does the institution originate/receive international ACH transactions? *Examiner note: International ACH transactions are potentially higher-risk and illegal transactions may be more difficult to monitor when initiated by an overseas entity.*			
A.3	Does the institution have any customers that have the characteristics of a third-party payment processor? *Examiner note: Refer to Figures 1 and 2. If the institution does not have any processor customers, the remaining questions are likely unnecessary.*			
A.4	Does the institution, as ODFI, allow any organization or person to have direct access to the ACH operator? *Examiner note: Granting another entity direct access requires strong controls and language in the agreement between the institution and the processor. This arrangement allows an entity to originate ACH transactions through the institution without authorization at the institution level. Entities that have direct access capability must be registered with NACHA as a Direct Access Participant. Direct access relationships should be reviewed closely, as described further in section C.6. Figure 4 explains this arrangement and other requirements.*			

	POLICY REVIEW *Examiner note: To complete this section, the examiner should reference the institution's written policies and procedures.*	**Y**	**N**	
B.1	Do the institution's policies and procedures:			
B.1a	• Outline thresholds for unauthorized returns and actions that may be imposed on processors that exceed those thresholds?			
B.1b	• Prescribe reporting requirements for the board of directors and management?			
B.1c	• Require adequate due diligence standards before taking on a TPPP customer, such as required background checks?			
B.1d	• Specify how management will remain aware of origination activity for the processor's customers?			
B.1e	• Specify how management will review the processor's compliance with applicable federal and state regulations?			

	MANAGEMENT PRACTICES & CONTROLS *Examiner note: This section is closely related to Section B: Policy Review. Management should be able to demonstrate adequate controls and a strong understanding of the risks, which begin with the development of strong policies and procedures.*			
C.1	Are controls and due diligence requirements in place that, at a minimum:			
C.1a	• Identify the major lines of business for the processor's customer(s)? *Examiner note: consider expanding the review if a processor's customers are unknown or exhibit the higher-risk characteristics described in Section A.*			
C.1b	• Require a review of the processor's policies, procedures, and processes to ensure the adequacy of *their* due diligence standards? *Examiner note: The degree to which*			

	processors are expected to perform due diligence on their customers should be specified in the agreement between the institution and processor. Refer to section D.3h below. Management should ensure that the processor has adequate processes in place to detect fraud or illegal transactions originated by its customers or a processor's customers.			
C.1c	• Include a review of the processor's corporate documentation and documentation on principal owners?[11]			
C.1d	• Include an initial onsite visit to the processor's operations center(s)?			
C.1e	• Control for the possibility that a processor re-sells its services to a third party that may act as agent?			
C.1f	• Provide for the review of the processor's management team to ensure no history of criminal activity or conflicts of interest exist between institution management and the processor management?			
C.1g	• Require payment processors to provide updated information on their merchant clients, such as names, principal business, location, and sales patterns, and the legality of their business operations?			
C.1h	• Provide for the submission of regular independent operational audits of the processor that assess the accuracy and reliability of the processor's systems?			
C.2	Has management put in place a system of monitoring account activity? *Examiner note: All activity should be monitored, not just closing balances. In some cases processors maintain consistent average daily balances, making the volume of debits and credits an equally important consideration.*			

[11] Some states require processors to license or register as a money service business or money transmitter. Operating a processor business without the necessary licenses or registrations is illegal in these states. An unregistered or unlicensed processor should be referred to the appropriate state regulatory agency(s).

C.3	Has management confirmed that the processor has the necessary licenses or registrations, if required by state law? *Examiner note: Many states have statutes that require processors to register as a money transmitter or a money service business (MSB). Federal law (18 U.S.C. § 1960(b) (1) (A)) prohibits the operation of a money transmitter business without the appropriate license in a state when such operation is punishable as a misdemeanor or felony under state law.*[12]			
C.4	Has management established that the processor has controls in place to monitor the return rates for its merchant customers? *Examiner note: Return rates may indicate high-risk origination practices, especially when the returns are due to unauthorized activity.*			
C.5	Has the institution verified the processor through public record databases *and* has the institution checked for state or federal regulatory actions or criminal actions against the merchant customers?			
C.6	For institutions that permit a processor to have direct access to the ACH operator, has management:			
C.6.a	• Ensured that all entities with direct access are registered their *Direct Access Debit* status with NACHA? *Examiner note: As part of the Direct Access Registration Rule, an ODFI must complete their registration by either: 1) acknowledging a statement to the effect that they have no direct access debit participants or 2) providing specific information about each Direct Access Debit Participant.*			
C.6.b	• Considered the arrangement separately in risk assessment processes?			

[12] Some states require processors to license or register as a money service business or money transmitter. Operating a processor business without the necessary licenses or registrations is illegal in these states. An unregistered or unlicensed processor should be referred to the appropriate state regulatory agency(s).

	CONTRACT & AGREEMENT REVIEW *Examiner note: A full legal review of the contracts between the processor and the institution is not outlined in the steps below. Instead, the steps below provide steps that help ensure management is maintaining an adequate contracting process. A more comprehensive set of procedures can be found in the ED Module: Third Party Risk. If responses indicate risk in this area, examiners are encouraged to expand the review using the ED Module.*			
D.1	Are contracts and/or agreements in writing and in place prior to the transaction of business between the parties?			
D.2	Does the board of directors and legal counsel provide approval of the contracts and/or agreements?			
D.3	Do contracts and/or agreements set forth the rights and responsibilities of each party, including:			
D.3a	• Timeframe covered by the contract?			
D.3b	• Requirement that the third party comply with all applicable laws, regulations, and regulatory guidance? *Examiner note: it is important management have the authority to terminate the contract if the processor is not compliant with all laws and regulations. See Section C for more information.*			
D.3c	• Authorization for the institution and appropriate state or federal regulators to have access to the records of the third party as necessary?			
D.3d	• Insurance coverage maintained by the third party?			
D.3e	• Permissibility or prohibition of the third party to subcontract or use another party to meet obligations?			
D.3f	• Indemnification or other compensation for contract violations?			
D.3g	• A provision that allows the institution to terminate the contract and/or agreement at any time?			
D.3h	• A requirement that processors establish and			

	perform their own customer due diligence procedures to ensure compliance with state licensing and registration statues and to detect fraud or illegal transactions? *Examiner note: See Section C for more information on licensing and registration statutes. It is important that the institution has the ability to terminate a contract if this requirement is not sufficiently met.*			
D.4	For institutions that permit a processor to have direct access to the ACH operator, do the contracts:			
D.4a	• Require that the party granted access obtain the institution's prior approval before originating ACH transactions under the institution's routing number?			
D.4b	• Specify limits established by the institution for files that the processor deposits with the ACH operator? *Examiner note: A file that exceeds these thresholds should be brought to the institution's attention before being deposited with the ACH Operator so the institution can approve it as an exception or require that it be held.*			
D.4c	• Include a provision that restricts the processor's ability to initiate correction files? *Examiner note: The institution should implement with the ACH Operator risk control measures that limit the correction ability of the party granted access. If institution management allows the other party to correct files, it should impose and enforce strict controls over these corrections. Specifically, management should first authorize any changes to the file totals and then instruct the ACH Operator to release the file for processing. This should be a positive check-off process; i.e., the ACH Operator should receive the authorization to process a file, and failure to receive the authorization should result in the file being deleted. In this way, the institution has control over its exposure from files processed by the other party.*			

	BANK SECRECY ACT & ANTI-MONEY LAUNDERING COMPLIANCE *Examiner note: The following procedures mirror those found in the most-recent FFIEC BSA/AML Examination Manual specific to payment processors. See the additional statement below for more information on BSA/AML compliance.*			
E.1	Are institution policy and procedures for monitoring customers, including third-party processors and their customers that utilize the ACH system, adequate given the size, complexity, location and type of customer relationship? Do procedures:			
E.1a	• Identify customers with frequent and large ACH transaction or international ACH activity?			
E.1b	• Monitor ACH detail activity when the batch-processed transactions are separated for other purposes (e.g., processing errors)?			
E.1c	• Apply increased, yet appropriate, due diligence requirements for higher-risk customers who originate or receive international ACH?			
E.1d	• Employ appropriate methods to track, review, and investigate consumer complaints or unauthorized returns regarding possible fraudulent or duplicate ACH transactions, including international ACH transactions?			
E.2	Has the institution filed any Suspicious Activity Reports (SARs) on any TPPP or any customer of a TPPP? *Examiner note: if answering "yes" above, review the SAR and determine whether any corrective action, if appropriate, was taken.*			
E.3	Can institution management demonstrate that the TPPP has an effective means of verifying merchant clients' identities and business practices, including the verification of an entity's OFAC status?			

Additional statement on BSA/AML compliance

The Bank Secrecy Act requires institutions to have BSA/AML compliance programs and appropriate policies, procedures, and processes in place to monitor and identify unusual activity, including ACH transactions. Obtaining customer due diligence (CDD) information on all operations is an important factor in mitigating BSA/AML risk in ACH transactions. Because of the nature of ACH transactions and the reliance that ODFIs and RDFIs place on each other for OFAC reviews and other necessary due diligence information, it is essential that all parties have a strong CDD program for regular ACH customers.

For relationships with processors, performing due diligence on the processor can be supplemented with due diligence on the processor's principals and, as necessary, on the originators. Adequate and effective CDD policies, procedures, and processes are critical in detecting a pattern of unusual and suspicious activities because the individual ACH transactions are typically not reviewed. Equally important is an effective risk-based suspicious activity monitoring and reporting system. In cases where an institution is heavily reliant upon the processor, an institution may want to review its suspicious activity monitoring and reporting program, either through its own or an independent inspection. The ODFI may establish an agreement with the TPPP that delineates general guidelines, such as compliance with ACH operating requirements and responsibilities and meeting other applicable state and federal regulations.

Regardless of the arrangement or number of parties to a transaction, responsibility for BSA/AML and OFAC compliance ultimately rests with the institution. The FDIC's Risk Management Manual states that,

> "Financial institutions are not permitted to transfer responsibility for OFAC compliance to correspondent institutions or a contracted third party, such as a data processing service provider. Each financial institution is responsible for every transaction occurring by or through its systems. If a sanctioned transaction transverses several U.S. financial institutions, all of these institutions will be subject to the same civil or criminal action, with the exception of the financial institution that blocked or rejected the transaction, as appropriate."

Institutions may need to consider controls to restrict or refuse ACH services to potential originators and receivers engaged in questionable or deceptive business practices.