Automated Clearing House Transactions — Overview

Objective. *Assess the adequacy of the bank's systems to manage the risks associated with automated clearing house (ACH) and international ACH transactions (IAT) and management's ability to implement effective monitoring and reporting systems.*

The use of the ACH has grown markedly over the last several years due to the increased volume of electronic check conversion[206] and one-time ACH debits, reflecting the lower cost of ACH processing relative to check processing.[207] Check conversion transactions, as well as one-time ACH debits, are primarily low-dollar value, consumer transactions for the purchases of goods and services or the payment of consumer bills. ACH is primarily used for domestic payments, but the Federal Reserve Banks' FedGlobal system[208] can currently accommodate cross-border payments to several countries around the world.

In September 2006, the Office of the Comptroller of the Currency issued guidance titled *Automated Clearinghouse Activities — Risk Management Guidance.* The document provides guidance on managing the risks of ACH activity. Banks may be exposed to a variety of risks when originating, receiving, or processing ACH transactions, or outsourcing these activities to a third party.[209]

ACH Payment Systems

Traditionally, the ACH system has been used for the direct deposit of payroll and government benefit payments and for the direct payment of mortgages and loans. As noted earlier, the ACH has been expanding to include one-time debits and check conversion. ACH transactions are payment instructions to either credit or debit a deposit account. Examples of credit payment transactions include payroll direct deposit, Social Security, dividends, and interest payments. Examples of debit transactions include mortgage, loan, insurance premium, and a variety of other consumer payments initiated through merchants or businesses.

In general, an ACH transaction is a batch-processed, value-dated, electronic funds transfer between an originating and a receiving bank. An ACH credit transaction is originated by the accountholder sending funds (payer), while an ACH debit transaction is originated by the

[206] In the electronic check conversion process, merchants that receive a check for payment do not collect the check through the check collection system, either electronically or in paper form. Instead, merchants use the information on the check to initiate a type of electronic funds transfer known as an ACH debit to the check writer's account. The check is used to obtain the bank routing number, account number, check serial number, and dollar amount for the transaction, and the check itself is not sent through the check collection system in any form as a payment instrument. Merchants use electronic check conversion because it can be a more efficient way for them to obtain payment than collecting the check.

[207] Refer to the NACHA Web site.

[208] The Federal Reserve Banks operate FedACH, a central clearing facility for transmitting and receiving ACH payments, and FedGlobal, which sends cross-border ACH credits payments to more than 35 countries around the world, plus debit payments to Canada only.

[209] Refer to OCC Bulletin 2006-39, "*Automated Clearing House Activities: Risk Management Guidance*" (September 1, 2006).

accountholder receiving funds (payee). 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 United States. A formal declaration of status as a Gateway is not required. ACH operators and ODFIs acting in the role of Gateways 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 Gateways may process outbound debit and credit entries, but can limit inbound entries to credit entries only and reversals.

International ACH Payments

NACHA —The Electronic Payments Association (NACHA) issued International ACH Transaction (IAT) operating rules and formats that became effective on September 18, 2009.[210] NACHA has since issued a number of modifications and refinements to their IAT operating rules. The IAT is a Standard Entry Class code for ACH payments that enables financial institutions to identify and monitor international ACH payments, and perform screening to ensure compliance with OFAC requirements. The rules require Gateways to classify payments that are transmitted to or received from a financial agency[211] outside the territorial jurisdiction of the United States as IATs. The classification depends on where the financial agency that handles the payment transaction (movement of funds) is located and not the location of any other party to the transaction (e.g., the Originator or Receiver).

Under NACHA operating rules, all U.S. financial institutions that participate in the ACH Network must be able to utilize the IAT format.

[210] For additional information on the IAT, refer to the NACHA Web site.

[211] "Financial agency" means an entity that is authorized by applicable law to accept deposits or is in the business of issuing money orders or transferring funds.

Definition of IAT

An IAT is an ACH entry that is part of a payment transaction involving a financial agency's office that is not located in the territorial jurisdiction of the United States. An office of a financial agency is involved in the payment transaction if one or more of the following conditions are met:

- Holds an account that is credited or debited as part of a payment transaction; or
- Receives funds directly from a person or makes payment directly to a person as part of a payment transaction; or
- Serves as an intermediary in the settlement of any part of a payment transaction.

IAT Defined Terms

An "inbound entry" originates in another country and is transmitted to the United States. For example, an inbound entry could be a customer's on-line purchase from an overseas vendor. An inbound entry could also be funding for a company payroll. Each subsequent IAT used for direct deposit would be an inbound IAT entry.

An "outbound entry" originates in the United States and is transmitted to another country. For example, IAT pension payments going from a U.S. ODFI to a U.S. RDFI in which the funds are then transferred to an account in another country would be outbound IAT entries.

Payment Transaction Guidance

A payment transaction is:

- An instruction of a sender to a bank to pay, or to obtain payment of, or to cause another bank to pay or to obtain payment of, a fixed or determinate amount of money that is to be paid to, or obtained from, a Receiver, and
- Any and all settlements, accounting entries, or disbursements that are necessary or appropriate to carry out the instruction.

Identification of IAT Parties

The NACHA operating rules define parties as part of an IAT entry:

- Foreign Correspondent Bank: A participating depository financial institution (DFI) that holds deposits owned by other financial institutions and provides payment and other services to those financial institutions.
- Foreign Gateway: A Gateway that acts as an entry point to or exit point from a foreign country.

Information Available Under the IAT Format

Data available to banks under the IAT format may assist banks in their OFAC, anti-money laundering, and monitoring efforts.[212] Originator and receiver information available to banks under the IAT format include:

- Originator name and address.
- Receiver name and address.
- Originator and Receiver account numbers.
- ODFI name (inbound IAT, foreign DFI), identification number, and branch country code.
- RDFI name (outbound IAT, foreign DFI), identification number, and branch country code.
- Country code.
- Currency code.
- Foreign Exchange indicator.

Effective March 14, 2014, a Gateway must identify within an inbound IAT entry:

- The ultimate foreign beneficiary of the funds transfer when the proceeds from a debit inbound IAT entry are "for further credit to" an ultimate foreign beneficiary that is other than the Originator of the debit IAT entry, or
- The foreign party funding a credit inbound IAT entry when that party is not the Originator of the credit IAT entry.

Refer to www.nacha.org/c/IATIndustryInformation.cfmfor more information on additional data available to banks under the new IAT format.

Third-Party Service Providers

A third-party service provider (TPSP) is an entity other than an Originator, ODFI, or RDFI that performs any functions on behalf of the Originator, the ODFI, or the RDFI with respect to the processing of ACH entries. For example, a bank may hire a TPSP to conduct ACH activities on behalf of the bank.[213] NACHA operating rules define TPSPs and relevant subsets of TPSPs that include "Third-Party Senders" and "Sending Points."[214] A third-party

[212] For convenience, this information is sometimes referred to as "Travel Rule" information, but as a technical matter the funds transfer recordkeeping and travel rules at 31 CFR 1010.410(f)) do not apply to ACH transactions and NACHA operating rules have not changed.

[213] Third-party service provider is a generic term for any business that provides services to a bank. A third-party payment processor is a specific type of service provider that processes payments such as checks, ACH files, or credit and debit card messages or files. Refer to expanded overview section, "Third-Party Payment Processors," page 234, for additional guidance.

[214] When independent TPSPs contract with independent sales organizations or other third-party payment processors, there may be two or more layers between the ODFI and the Originator.

sender is a type of service provider that acts on behalf of an Originator (i.e., an intermediary between the Originator and the ODFI). For example, a third-party sender may be a customer of the bank processing ACH transactions on behalf of an Originator. In a third-party sender arrangement, there is no contractual agreement between the ODFI and the Originator. A sending point is defined as an entity that transmits entries to an ACH Operator on behalf of an ODFI.

The functions of these TPSPs can include, but are not limited to, the creation of ACH files on behalf of the Originator or ODFI, or acting as a sending point of an ODFI (or receiving point on behalf of an RDFI).

Risk Factors

The ACH system was designed to transfer a high volume of low-dollar domestic transactions, which pose lower BSA/AML risks. Nevertheless, the ability to send high-dollar and international transactions through the ACH may expose banks to higher BSA/AML risks. Banks without a robust BSA/AML monitoring system may be exposed to additional risk particularly when accounts are opened over the Internet without face-to-face contact.

ACH transactions that are originated through a TPSP (that is, when the Originator is not a direct customer of the ODFI) may increase BSA/AML risks, therefore, making it difficult for an ODFI to underwrite and review Originator transactions for compliance with BSA/AML rules.[215] Risks are heightened when neither the TPSP nor the ODFI performs due diligence on the companies for whom they are originating payments.

Certain ACH transactions, such as those originated through the Internet or the telephone, may be susceptible to manipulation and fraudulent use. Certain practices associated with how the banking industry processes ACH transactions may expose banks to BSA/AML risks. These practices include:

- An ODFI authorizing a TPSP 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.
- Lack of sharing of information on or about originators and receivers inhibits a bank's ability to appropriately assess and manage the risk associated with correspondent and ACH processing operations, monitor for suspicious activity, and screen for OFAC compliance.

[215] A bank's underwriting policy should define what information each application should contain. The depth of the review of an originator's application should match the level of risk posed by the originator. The underwriting policy should require a background check of each originator to support the validity of the business.

Risk Mitigation

The BSA requires banks to have BSA/AML compliance programs and appropriate policies, procedures, and processes in place to monitor and identify unusual activity, including ACH transactions. Obtaining CDD information in all operations is an important mitigant of 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 TPSPs, CDD on the TPSP can be supplemented with due diligence on the principals associated with the TPSP 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 a bank is heavily reliant upon the TPSP, a bank may want to review the TPSP's suspicious activity monitoring and reporting program, either through its own or an independent inspection. The ODFI may establish an agreement with the TPSP, which delineates general TPSP guidelines, such as compliance with ACH operating requirements and responsibilities and meeting other applicable state and federal regulations. Banks may need to consider controls to restrict or refuse ACH services to potential originators and receivers engaged in questionable or deceptive business practices.

ACH transactions can be used in the layering and integration stages of money laundering. Detecting unusual activity in the layering and integration stages can be a difficult task, because ACH may be used to legitimize frequent and recurring transactions. Banks should consider the layering and integration stages of money laundering when evaluating or assessing the ACH transaction risks of a particular customer.

The ODFI should be aware of IAT activity and evaluate the activity using a risk-based approach in order to ensure that suspicious activity is identified and monitored. The ODFI, if frequently involved in IATs, may develop a separate process, which may be automated, for reviewing IATs that minimizes disruption to general ACH processing, reconcilement, and settlement.

The potentially higher risk inherent in IATs should be considered in the bank's ACH policies, procedures, and processes. The bank should consider its current and potential roles and responsibilities when developing internal controls to monitor and mitigate the risk associated with IATs and to comply with the bank's suspicious activity reporting obligations.

In processing IATs, banks should consider the following:

- Customers and transactions types and volume.
- Third-party payment processor relationships.
- Responsibilities, obligations, and risks of becoming a Gateway.
- CIP, CDD, and EDD standards and practices.
- Suspicious activity monitoring and reporting.

- Appropriate MIS, including the potential necessity for systems upgrades or changes.
- Processing procedures (e.g., identifying and handling IATs, resolving OFAC hits, and handling noncompliant and rejected messages).
- Training programs for appropriate bank personnel (e.g., ACH personnel, operations, compliance audit, customer service, etc.).
- Legal agreements, including those with customers, third-party processors, and vendors, and whether those agreements need to be upgraded or modified.

OFAC Screening

ACH transactions may involve persons or parties that are subject to the sanctions programs administered by OFAC. (Refer to core overview section, "Office of Foreign Assets Control," page 142, for additional guidance.) OFAC has clarified its interpretation of the application of its rules for domestic and cross-border ACH transactions and provided more detailed guidance on cross-border ACH.[216]

With respect to domestic ACH transactions, the ODFI is responsible for verifying that the Originator is not a blocked party and making a good faith effort to ascertain that the Originator is not transmitting blocked funds. The RDFI similarly is responsible for verifying that the Receiver is not a blocked party. In this way, the ODFI and the RDFI are relying on each other for compliance with OFAC regulations.

If an ODFI receives domestic ACH transactions that its customer has already batched, the ODFI is not responsible for unbatching those transactions to ensure that no transactions violate OFAC's regulations. If an ODFI unbatches a file originally received from the Originator in order to process "on-us" transactions, that ODFI is responsible for the OFAC compliance for the on-us transactions because it is acting as both the ODFI and the RDFI for those transactions. ODFIs acting in this capacity should already know their customers for the purpose of compliance with OFAC and other regulatory requirements. For the residual unbatched transactions in the file that are not "on-us," as well as those situations where banks deal with unbatched ACH records for reasons other than to strip out the on-us transactions, banks should determine the level of their OFAC risk and develop appropriate policies, procedures, and processes to address the associated risks. Such policies might involve screening each unbatched ACH record. Similarly, banks that have relationships with TPSP should assess the nature of those relationships and their related ACH transactions to ascertain the bank's level of OFAC risk and to develop appropriate policies, procedures, and processes to mitigate that risk.

With respect to cross-border screening, similar but somewhat more stringent OFAC screening obligations hold for IATs. In the case of inbound IATs, and regardless of whether the OFAC flag in the IAT is set, an RDFI is responsible for compliance with OFAC sanctions. For outbound IATs, the ODFI should not rely on OFAC screening by an RDFI outside of the United States. In these situations, the ODFI must exercise increased diligence to ensure that illegal transactions are not processed.

[216] Refer to Interpretive Note 041214-FACRL-GN-02.

Due diligence for an inbound or outbound IAT may include screening the parties to a transaction, as well as reviewing the details of the payment field information for an indication of a sanctions violation, investigating the resulting hits, if any, and ultimately blocking or rejecting the transaction, as appropriate. Refer to the core overview section, "Office of Foreign Asset Control," page 142, for additional guidance.

In guidance issued on March 10, 2009, OFAC authorized institutions in the United States when they are acting as an ODFI/Gateway for inbound IAT debits to reject transactions that appear to involve blockable property or property interests.[217] The guidance further stated that to the extent that an ODFI/Gateway screens inbound IAT debits for possible OFAC violations prior to execution and in the course of such screening discovers a potential OFAC violation, the suspect transaction is to be removed from the batch for further investigation. If the ODFI/Gateway determines that the transaction does appear to violate OFAC regulations, the ODFI/Gateway should refuse to process the transfer. The procedure applies to transactions that would normally be blocked as well as to transactions that would normally be rejected for OFAC purposes based on the information in the payments.

Additional information on the types of retail payment systems (ACH payment systems) is available in the FFIEC *Information Technology Examination Handbook's* *Retail Payment Systems* booklet.

[217] Refer to OFAC letter (March 10, 2009).