Funds Transfers — Overview

Objective. *Assess the adequacy of the bank's systems to manage the risks associated with funds transfers, and management's ability to implement effective monitoring and reporting systems. This section expands the core review of the statutory and regulatory requirements of funds transfers to provide a broader assessment of AML risks associated with this activity.*

Payment systems in the United States consist of numerous financial intermediaries, financial services firms, and nonbank businesses that create, process, and distribute payments. The domestic and international expansion of the banking industry and nonbank financial services has increased the importance of electronic funds transfers, including funds transfers made through the wholesale payment systems. Additional information on the types of wholesale payment systems is available in the FFIEC *Information Technology Examination Handbook.*[200]

Funds Transfer Services

The vast majority of the value of U.S. dollar payments, or transfers, in the United States is ultimately processed through wholesale payment systems, which generally handle large-value transactions between banks. Banks conduct these transfers on their own behalf as well as for the benefit of other financial service providers and bank customers, both corporate and consumer.

Related retail transfer systems facilitate transactions such as automated clearing houses (ACH); automated teller machines (ATM); point-of-sales (POS);, telephone bill paying; home banking systems; and credit, debit, and prepaid cards. Most of these retail transactions are initiated by customers rather than by banks or corporate users. These individual transactions may then be batched in order to form larger wholesale transfers, which are the focus of this section.

The two primary domestic wholesale payment systems for interbank funds transfers are the Fedwire Funds Service (Fedwire®)[201] and the Clearing House Interbank Payments System (CHIPS).[202] The bulk of the dollar value of these payments is originated electronically to make large value, time-critical payments, such as the settlement of interbank purchases and sales of federal funds, settlement of foreign exchange transactions, disbursement or repayment of loans; settlement of real estate transactions or other financial market transactions; and purchasing, selling, or financing securities transactions. Fedwire and CHIPS participants facilitate these transactions on their behalf and on behalf of their customers, including nonbank financial institutions, commercial businesses, and correspondent banks that do not have direct access.

Structurally, there are two components to funds transfers: the instructions, which contain information on the sender and receiver of the funds, and the actual movement or transfer of

[200] Refer to the FFIEC *Information Technology Examination Handbook*.

[201] Fedwire® Services is a registered service mark of the Federal Reserve Banks.

[202] CHIPS is a private multilateral settlement system owned and operated by The Clearing House Payments Co., LLC.

funds. The instructions may be sent in a variety of ways, including by electronic access to networks operated by the Fedwire or CHIPS payment systems; by access to financial telecommunications systems, such as Society for Worldwide Interbank Financial Telecommunication (SWIFT); or e-mail, facsimile, telephone, or telex. Fedwire and CHIPS are used to facilitate U.S. dollar transfers between two domestic endpoints or the U.S. dollar segment of international transactions. SWIFT is an international messaging service that is used to transmit payment instructions for the vast majority of international interbank transactions, which can be denominated in numerous currencies.

Fedwire

Fedwire is operated by the Federal Reserve Banks and allows a participant to transfer funds from its master account at the Federal Reserve Banks to the master account of any other bank.[203] Payment over Fedwire is final and irrevocable when the Federal Reserve Bank either credits the amount of the payment order to the receiving bank's Federal Reserve Bank master account or sends notice to the receiving bank, whichever is earlier. Although there is no settlement risk to Fedwire participants, they may be exposed to other risks, such as errors, omissions, and fraud.

Participants may access Fedwire by three methods:

- Direct mainframe-to-mainframe (Fedline Direct).
- Internet access over a virtual private network to Web-based applications (FedLine Advantage).
- Off-line or telephone-based access to a Federal Reserve Bank operations site.

CHIPS

CHIPS is a privately operated, real-time, multilateral payments system typically used for large-dollar payments. CHIPS is owned by banks, and any banking organization with a regulated U.S. presence may become a participant in the system. Banks use CHIPS for the settlement of both interbank and customer transactions, including, for example, payments associated with commercial transactions, bank loans, and securities transactions. CHIPS also plays a large role in the settlement of USD payments related to international transactions, such as foreign exchange, international commercial transactions, and offshore investments.

[203] An entity eligible to maintain a master account at the Federal Reserve is generally eligible to participate in the Fedwire Funds Service. These participants include:

- Depository institutions.
- U.S. agencies and branches of foreign banks.
- Member banks of the Federal Reserve System.
- The U.S. Treasury and any entity specifically authorized by federal statute to use the Federal Reserve Banks as fiscal agents or depositories.
- Entities designated by the Secretary of the Treasury.
- Foreign central banks, foreign monetary authorities, foreign governments, and certain international organizations.
- Any other entity authorized by a Federal Reserve Bank to use the Fedwire Funds Service.

Continuous Linked Settlement (CLS) Bank

CLS Bank is a private-sector, special-purpose bank that settles simultaneously both payment obligations that arise from a single foreign exchange transaction. The CLS payment-versus-payment settlement model ensures that one payment segment of a foreign exchange transaction is settled if and only if the corresponding payment segment is also settled, eliminating the foreign exchange settlement risk that arises when each segment of the foreign exchange transaction is settled separately. CLS is owned by global financial institutions through shareholdings in CLS Group Holdings AG, a Swiss company that is the ultimate holding company for CLS Bank. CLS Bank currently settles payment instructions for foreign exchange transactions in 17 currencies and is expected to add more currencies over time.

SWIFT

The SWIFT network is a messaging infrastructure, not a payments system, which provides users with a private international communications link among themselves. The actual funds movements (payments) are completed through correspondent bank relationships, Fedwire, or CHIPS. Movement of payments denominated in different currencies occurs through correspondent bank relationships or over funds transfer systems in the relevant country. In addition to customer and bank funds transfers, SWIFT is used to transmit foreign exchange confirmations, debit and credit entry confirmations, statements, collections, and documentary credits.

Cover Payments

A typical funds transfer involves an originator instructing its bank (the originator's bank) to make payment to the account of a payee (the beneficiary) with the beneficiary's bank. A cover payment occurs when the originator's bank and the beneficiary's bank do not have a relationship that allows them to settle the payment directly. In that case, the originator's bank instructs the beneficiary's bank to effect the payment and advises that transmission of funds to "cover" the obligation created by the payment order has been arranged through correspondent accounts at one or more intermediary banks.

Cross-border cover payments usually involve multiple banks in multiple jurisdictions. For U.S. dollar transactions, the intermediary banks are generally U.S. banks that maintain correspondent banking relationships with non-U.S. originators' banks and beneficiaries' banks. In the past, SWIFT message protocols allowed cross-border cover payments to be effected by the use of separate, simultaneous message formats:

- The MT 103 — payment order from the originator's bank to the beneficiary's bank with information identifying the originator and the beneficiary; and
- The MT 202 — bank-to-bank payment orders directing the intermediary banks to "cover" the originator's bank's obligation to pay the beneficiary's bank.

To address transparency concerns, SWIFT adopted a new message format for cover payments (the MT 202 COV) that contains mandatory fields for originator and beneficiary information. Effective November 21, 2009, the MT 202 COV is required for any bank-to-bank payment for which there is an associated MT 103. The MT 202 COV provides

intermediary banks with additional originator and beneficiary information to perform sanctions screening and suspicious activity monitoring. The introduction of the MT 202 COV does not alter a U.S. bank's OFAC or BSA/AML obligations.

The MT 202 format remains available for bank-to-bank funds transfers that have no associated MT 103 message. For additional detail about transparency in cover payments, refer to *Transparency and Compliance for U.S. Banking Organizations Conducting Cross-Border Funds Transfers* (December 18, 2009), which can be found at each federal banking agencies' Web site.

Informal Value Transfer Systems

An informal value transfer system (IVTS) (e.g., hawalas) is a term used to describe a currency or value transfer system that operates informally to transfer money as a business.[204] In countries lacking a stable financial sector or with large areas not served by formal banks, IVTS may be the only method for conducting financial transactions. Persons living in the United States may also use IVTS to transfer funds to their home countries.

IVTS may legally operate in the United States as a Money Services Business, and specifically as a type of money transmitter, so long as they abide by applicable state and federal laws. This includes registering with FinCEN and complying with BSA/AML provisions applicable to all money transmitters. A more sophisticated form of IVTS operating in the United States often interacts with other financial institutions in storing currency, clearing checks, remitting and receiving funds, and obtaining other routine financial services, rather than acting independently of the formal financial system.

Payable Upon Proper Identification Transactions

One type of funds transfer transaction that carries particular risk is the payable upon proper identification (PUPID) service. PUPID transactions are funds transfers for which there is no specific account to deposit the funds into and the beneficiary of the funds is not a bank customer. For example, an individual may transfer funds to a relative or an individual who does not have an account relationship with the bank that receives the funds transfer. In this case, the beneficiary bank may place the incoming funds into a suspense account and ultimately release the funds when the individual provides proof of identity. In some cases, banks permit noncustomers to initiate PUPID transactions. These transactions are considered extremely high risk and require strong controls.

[204] Sources of information on IVTS include:

- FinCEN Advisory FIN-2010-A011, *Informal Value Transfer Systems*, September 2010
- FinCEN Advisory 33, *Informal Value Transfer Systems*, March 2003.
- U.S. Treasury *Informal Value Transfer Systems Report to the Congress in Accordance with Section 359 of the Patriot Act*, November 2002.
- Financial Action Task Force on Money Laundering (FATF), *Interpretative Note to Special Recommendation VI: Alternative Remittance*, June 2003.
- FATF, *Combating the Abuse of Alternative Remittance Systems, International Best Practices*, October 2002.

Risk Factors

Funds transfers may present a heightened degree of risk, depending on such factors as the number and dollar volume of transactions, geographic location of originators and beneficiaries, and whether the originator or beneficiary is a bank customer. The size and complexity of a bank's operation and the origin and destination of the funds being transferred determine which type of funds transfer system the bank uses. The vast majority of funds transfer instructions are conducted electronically; however, examiners need to be mindful that physical instructions may be transmitted by other informal methods, as described earlier.

Cover payments effected through SWIFT pose additional risks for an intermediary bank that does not receive either a MT 103 or an adequately completed MT 202 COV that identifies the originator and beneficiary of the funds transfer. Without this data, the intermediary bank is unable to monitor or filter payment information. This lack of transparency limits the U.S. intermediary bank's ability to appropriately assess and manage the risk associated with correspondent and clearing operations, monitor for suspicious activity, and screen for OFAC compliance.

IVTS pose a heightened concern because they are able to circumvent the formal system. The lack of recordkeeping requirements coupled with the lack of identification of the IVTS participants may attract money launderers and terrorists. IVTS also pose heightened BSA/AML concerns because they can evade internal controls and monitoring oversight established in the formal banking environment. Principals that operate IVTS frequently use banks to settle accounts.

The risks of PUPID transactions to the beneficiary bank are similar to other activities in which the bank does business with noncustomers. However, the risks are heightened in PUPID transactions if the bank allows a noncustomer to access the funds transfer system by providing minimal or no identifying information. Banks that allow noncustomers to transfer funds using the PUPID service pose significant risk to both the originating and beneficiary banks. In these situations, both banks have minimal or no identifying information on the originator or the beneficiary.

Risk Mitigation

Funds transfers can be used in the placement, layering, and integration stages of money laundering. Funds transfers purchased with currency are an example of the placement stage. Detecting unusual activity in the layering and integration stages is more difficult for a bank because transactions may appear legitimate. In many cases, a bank may not be involved in the placement of the funds or in the final integration, only the layering of transactions. Banks should consider all three stages of money laundering when evaluating or assessing funds transfer risks.

Banks need to have sound policies, procedures, and processes to manage the BSA/AML risks of its funds transfer activities. Such policies may encompass more than regulatory recordkeeping minimums and be expanded to cover OFAC obligations. Funds transfer policies, procedures, and processes should address all foreign correspondent banking activities, including transactions in which U.S. branches and agencies of foreign banks are intermediaries for their head offices.

Obtaining CDD information is an important risk mitigation step in providing funds transfer services. Because of the nature of funds transfers, adequate and effective CDD policies, procedures, and processes are critical in detecting unusual and suspicious activities. An effective risk-based suspicious activity monitoring and reporting system is equally important. Whether this monitoring and reporting system is automated or manual, it should be sufficient to detect suspicious trends and patterns typically associated with money laundering.

Institutions should have processes for managing correspondent banking relationships in accordance with section 312 of the USA PATRIOT Act and corresponding regulations (31 CFR 1010.610). Correspondent bank due diligence should take into account the correspondent's practices with regard to funds transfers effected through the U.S. bank.

U.S. banks can mitigate risk associated with cover payments by managing correspondent banking relationships, by observing The Clearing House Payments Co., LLC and the Wolfsberg Group's best practices (discussed below) and the SWIFT standards when sending messages, and by conducting appropriate transaction screening and monitoring.

In May 2009, the Basel Committee on Banking Supervision issued a paper on cross-border cover payment messages (BIS Cover Payments Paper).[205] The BIS Cover Payments Paper supported increased transparency and encouraged all banks involved in international payments transactions to adhere to the message standards developed by The Clearing House Payments Co., LLC and the Wolfsberg Group in 2007. These are:

- Financial institutions should not omit, delete, or alter information in payment messages or orders for the purpose of avoiding detection of that information by any other financial institution in the payment process;
- Financial institutions should not use any particular payment message for the purpose of avoiding detection of information by any other financial institution in the payment process;
- Subject to all applicable laws, financial institutions should cooperate as fully as practicable with other financial institutions in the payment process when requested to provide information about the parties involved; and
- Financial institutions should strongly encourage their correspondent banks to observe these principles.

In addition, effective monitoring processes for cover payments include:

- Monitoring funds transfers processed through automated systems in order to identify suspicious activity. This monitoring may be conducted after the transfers are processed, on an automated basis, and may use a risk-based approach. The MT 202 COV provides intermediary banks with useful information, which can be filtered using risk factors

[205] Refer to the Basel Committee on Banking Supervision's *Due diligence and transparency regarding cover payment messages related to cross-border wire transfers*. In addition, during August 2009, the committee, along with the Clearinghouse Payments Co. LLC, released Q&As in order to enhance understanding of the MT 202 COV.

developed by the intermediary bank. The monitoring process may be similar to that for MT 103 payments.

- Given the volume of messages and data for large U.S. intermediary banks, a manual review of every payment order may not be feasible or effective. However, intermediary banks should have, as part of their monitoring processes, a risk-based method to identify incomplete fields or fields with meaningless data. U.S. banks engaged in processing cover payments should have policies to address such circumstances, including those that involve systems other than SWIFT.

Originating and beneficiary banks should establish effective and appropriate policies, procedures, and processes for PUPID activity including:

- Specifying the type of identification that is acceptable.
- Maintaining documentation of individuals consistent with the bank's recordkeeping policies.
- Defining which bank employees may conduct PUPID transactions.
- Establishing limits on the amount of funds that may be transferred to or from the bank for noncustomers (including type of funds accepted (i.e., currency or official check) by originating bank).
- Monitoring and reporting suspicious activities.
- Providing enhanced scrutiny for transfers to or from certain jurisdictions.
- Identifying disbursement method (i.e., by currency or official check) for proceeds from a beneficiary bank.