The Clearing House®

At the Center of Banking Since 1853®

Guiding Principles for Anti-Money Laundering Policies and Procedures in Correspondent Banking

February 2016

Executive Summary

The Clearing House Association, L.L.C. ("The Clearing House") published its *Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking* in March 2002 (the "2002 Guidelines"). The 2002 Guidelines were intended to provide guidance to U.S. banks engaged in foreign correspondent banking and to assist U.S. banks in implementing the anti-money laundering ("AML") requirements of Section 312 of the USA PATRIOT Act of 2001 (31 U.S.C. 5318(i)) (the "PATRIOT Act"). Section 312 requires covered financial institutions to implement AML policies, procedures and controls for foreign correspondent banking.

In light of changes in statutes and regulations, increased supervisory expectations and heightened regulatory scrutiny of correspondent banking in the United States since the publication of The Clearing House's original guidelines in 2002, The Clearing House believes that it is important to update the principles that address these changes, incorporate industry practice as it has evolved, and recognize the different roles and responsibilities of each institution in the payment process. Therefore, in 2014, The Clearing House published an exposure draft of these principles, with comments received on that draft incorporated into this final, updated 2016 version.

The Clearing House recognizes its responsibility to adopt and continually improve AML policies, procedures and controls that are reasonably designed to be both operational and effective, including procedures for detecting and reporting payments that involve suspicious activity that could be related to money laundering or other financial crimes. Therefore,The Clearing House is publishing the following updated guiding principles for sound business conduct in correspondent banking (the "Guiding Principles") to supplement the fight against money laundering and other financial crimes and to assist U.S. banks in complying with the PATRIOT Act and its implementing regulations.

Since the 2002 Guidelines were published, the U.S. Department of the Treasury and U.S. bank regulators promulgated detailed regulations under Section 312 of the PATRIOT Act. Those regulations clarified that the Section 312 requirements apply not just to traditional correspondent accounts maintained for foreign banks for the purpose of payment processing, but to any formal relationship through which the financial institution provides regular services to any foreign financial institution, which may include, for banks, demand deposit, savings deposit or other transaction or asset accounts, and credit accounts or other extensions of credit.

Table of Contents

I. Introduction

These Guiding Principles focus on traditional correspondent banking involving payment processing for foreign banks (other than ACH), such as funds transfers, cash letters and pouch activity, and bulk cash, and they do not address institutional brokerage and capital market activities, trade finance or lending, or activities engaged in for nonbank financial institutions, such as brokerage firms and money service businesses. These principles are intended to address the policies and procedures applicable to all foreign correspondent banking customers, including affiliates, subsidiaries or branches of the bank.

The Guiding Principles are intended to build upon a U.S. bank's existing AML program and to assist the U.S. bank in the continuing redesign and development of comprehensive due diligence programs to identify and manage particular risks that may exist. Sound risk management policies and procedures vary among banks and, therefore, the application of the Guiding Principles also may vary among such banks.[1]

Since publication of the 2002 Guidelines, industry standards have progressed to reflect the industry's enhanced understanding of the money laundering risks associated with correspondent accounts and to meet the evolving regulatory requirements and expectations. Advancements in technology have enhanced banks' capabilities to monitor transactions of their foreign correspondent banking customers and raised expectations of regulators and law enforcement authorities with regard to banks' responsibilities to identify suspicious activity flowing through their customers' accounts.

1 Refer to Appendix A for definitions to the terms used herein.

International standards for transparency in payment messages have also advanced with the publication of the "Statement on Payment Message Standards" by the Wolfsberg Group and The Clearing House Association and other regulatory guidance as well as the introduction of the SWIFT MT 202 COV.[2]

What has not changed since 2002, however, is that correspondent banking, whereby banks around the world can make payments to and through each other, continues to be an integral part of the international payment system. Correspondent banking fosters economic prosperity throughout the world by enabling business and remittance flows between countries. Without having to maintain branches in every country, banks can utilize their relationships with other banks to serve their customers' global payment needs with the essential attributes of confidence, speed and efficiency.

These very attributes, which are so instrumental to the successful functioning of the payment system, however, also create vulnerability to money laundering. The volume of payments, the speed at which payments must move, and the fungibility of payments combine to make it virtually impossible to identify and intercept payments unless the originator, the beneficiary

2 The Wolfsberg Group & The Clearing House Association Statement on Payment Message Standards, available at: http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_NYCH_Statement_on_Payment_Message_Standards_(2007).pdf (Apr. 19, 2007); Basel Committee on Banking Supervision: Due diligence and transparency regarding cover payment messages related to cross-border wire transfers, available at: http://www.bis.org/publ/bcbs154.htm (May 2009); Transparency and Compliance for U.S. Banking Organizations Conducting Cross-Border Funds Transfers, available at: http://www.occ.gov/news-issuances/bulletins/2009/bulletin-2009-36.html (Dec. 18, 2009).

or the financial institutions involved in the payment are identified as problematic in advance and are clearly identified in the payment order. Once a person is able to inject funds into the payment system that are the product of a criminal act, are intended to finance a criminal act, or are tied to a party subject to U.S. sanctions, it is very difficult, and in many cases impossible, to identify those funds as they move from bank to bank. Similarly, the scope necessary for an effective payment system requires broad availability and thereby greatly limits the feasibility of blanket exclusions based on geography or origin. It is therefore essential that payment instructions be transparent so banks can take preventative and cautionary measures. These measures, however, can by their nature be effective only if all parties to the transaction, including the originator, beneficiary and other financial institutions involved in the payment process are clearly identified in the payment order received by the bank. If banks sending payments through the system are engaged in deceptive practices, it can be almost impossible for correspondent banks to detect. Government cooperation in setting and enforcing international standards for anti-money laundering and transparency in the financial system is essential if banks' efforts to detect and report potential money laundering are to be effective.

1. REGULATORY DEVELOPMENTS

In December 2002, the Treasury promulgated regulations implementing Sections 313/319 of the PATRIOT Act (31 U.S.C. § 5318(j)-(k)).[3] These regulations implement the PATRIOT Act's prohibition on U.S. banks maintaining correspondent accounts in the United States for foreign shell banks (i.e., banks that do not have any physical presence and are not regulated affiliates) and U.S. banks take reasonable steps to ensure that foreign banks are not using their correspondent accounts to indirectly provide banking services to any such foreign shell banks. These regulations also require that U.S. banks obtain ownership information for foreign banks whose shares are not publicly traded, as well as the name and address of an agent in the United States designated to accept service of legal process for the foreign bank.

In 2006 and 2007, the Treasury promulgated regulations implementing Section 312 of the PATRIOT Act (31 U.S.C. § 5318(i)).[4] Among other things, these regulations apply the PATRIOT Act's requirements related to "correspondent accounts" broadly to accounts maintained at U.S. banks held for foreign financial institutions. Specifically, the regulations require that banks apply risk-based due diligence policies, procedure and controls to its correspondent accounts maintained in the United States for foreign financial institutions. The regulations also require that banks undertake enhanced due diligence ("EDD") with respect to accounts established or maintained for certain higher risk foreign banks.

In addition to these regulations implementing Sections 312, 313 and 319 of the PATRIOT Act, the U.S. Government has provided guidance clarifying its expectations with respect to a U.S. bank's AML policies and procedures in correspondent banking. For example, in March 2010, the Federal Financial Institutions Examination Council ("FFIEC") issued an updated publication of the "Bank Secrecy Act/Anti-Money Laundering Examination Manual" (FFIEC BSA/AML Examination Manual" or "FFIEC Manual") which describes U.S. federal bank-

3 31 CFR § 1010.630.

4 31 CFR § 1010.610.

ing regulators' expectations with respect to, among other things, a U.S. bank's due diligence and recordkeeping requirements relating to its maintenance of correspondent accounts in the United States for foreign financial institutions. Also notably, on August 4, 2014, the Treasury issued a notice of proposed rulemaking on customer due diligence ("CDD") requirements for financial institutions (79 Federal Register 45151 (August 4, 2014)). International organizations, such as the Financial Action Task Force ("FATF"), have also increased their focus on correspondent banking (FATF Recommendation 13 on correspondent banking as part of its 40 Recommendations in its "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation").

AML measures for correspondent banking have, in recent years, been a subject of increased supervisory focus. Another area of increased focus has been sanctions risk—risk that correspondent banking may provide persons subject to U.S. sanctions indirect access to the U.S. financial system. In this regard, much has been done in the last decade by the U.S. government and international bodies, as well as the financial industry itself, to address these risks.

In conjunction with heightened regulatory expectations, U.S. banking regulators, as well as U.S. law enforcement agencies, have increased their scrutiny of AML measures and sanctions compliance in the correspondent banking operations of U.S. and international financial institutions. The combination of increased scrutiny and elevated expectations has contributed to a proliferation of bank regulatory and law enforcement actions related to correspondent banking activities. These range from informal corrective programs mandated by regulators, to formal regulatory enforcement actions, civil money penalties and, in some cases, criminal prosecution.

Sanctions-related enforcement actions have highlighted the importance of transparency in funds transfers in particular and in the payments system in general. As part of an initiative to address the risks related to transparency in international payments, The Clearing House, in conjunction with the Wolfsberg Group, developed standards to which all banks involved in international payments transactions are encouraged to adhere. These standards were endorsed by the Basel Committee on Banking Supervision and included in guidance from the FFIEC. Additionally, SWIFT developed a new payment instruction format, the MT 202 COV, which must be used for any bank-to-bank transfer that is a cover payment. Information relating to the originator and beneficiary is mandatory in the MT 202 COV.

The sanctions laws in the United States with regard to correspondent accounts held at banks in the United States for foreign banks were significantly enhanced by the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 ("CISADA"), which has affected banks' treatment of correspondent accounts maintained by foreign banks, in particular, with regard to their performance of due diligence and monitoring of correspondent accounts.

2. ROLES OF BANKS

With respect to any cross-border payment made by a foreign correspondent bank customer on behalf of its customer through its U.S. correspondent account, each bank in the payment process—originator's bank, intermediary banks and beneficiary's bank—plays a different role and therefore has a different level

of visibility into the parties and the purpose of the payment. The intermediary bank generally has limited or no understanding of the originator or beneficiary, their ordinary account activity or the purpose of the payment, while the originator's and beneficiary's banks are better positioned to understand the purpose of the payment, as well as the normal activity of the originator or beneficiary.

As a result, for each payment made through a correspondent account, the AML responsibilities and supervisory expectations of the originator's bank, the intermediary bank(s) and the beneficiary's bank differ. It is ordinarily not practicable to require the intermediary banks to conduct due diligence on, or even identify, the customers of the originator's and beneficiary's banks. They must depend on the due diligence of the originator's or beneficiary's bank. Indeed, the efficient functioning of the international payment system requires this dependence. In addition, it is the responsibility of the originator's bank to include complete and accurate information in the payment orders it sends to the intermediary and beneficiary's bank.

II. Anti-Money Laundering Policies and Procedures in Correspondent Banking

1. ESTABLISHMENT OF CORRESPONDENT ACCOUNTS

a. Account Opening

Prior to the opening of a Correspondent Account for a Foreign Bank, the Bank should conduct due diligence and, where appropriate based on its risk assessment of the Foreign Bank, enhanced due diligence with regard to the Foreign Bank.

b. The Application of a Bank's Customer Identification Program to Foreign Correspondent Banking Customers

All Banks must have a written customer identification program ("CIP") that implements Section 326 of the PATRIOT Act and its implementing regulation ("CIP Rule"), and enables the Bank to form a reasonable belief that it knows the true identity of its Foreign Correspondent Banking Customer. The Bank's CIP should specify appropriate account-opening procedures, detailing the minimum identifying information (i.e., name, address and identification number) the Bank should obtain from each prospective customer. The Bank should also implement reasonable and practical risk-based procedures for verifying the identity of each Foreign Correspondent Banking Customer by utilizing documentary or non-documentary verification methods. Documentary verification showing the legal existence of the entity may include certified articles of incorporation, or an unexpired government-issued business license (or evidence from a government website showing that the financial institution is licensed). Non-documentary verification methods may include, among others, the Bank contacting the customer, independently verifying the customer's identity through a comparison of information provided by the customer with information obtained from a public database or other source, checking references with other financial institutions and obtaining a financial statement.

Based on the Bank's risk assessment of a new correspondent banking customer, the Bank may decide to obtain information about the individuals with authority or control over the Correspondent Account, including signatories, in order to verify the customer's identity. This verification method may apply only when the Bank is unable to verify the customer's true identity through its use of documentary or non-documentary methods.

c. Due Diligence Programs for Foreign Correspondent Banking Customers

In addition to its obligations under the CIP Rule, the Bank is required under Section 312 of the PATRIOT Act to establish and maintain a due diligence program that includes appropriate, specific, risk-based and, where necessary, enhanced policies, procedures and controls that are reasonably designed to enable the Bank to detect and report, on an ongoing basis, any known or suspected money laundering activity

conducted through or involving any Correspondent Account established, maintained, administered or managed by the Bank in the United States for a foreign financial institution.

The Bank should develop and maintain risk-based enhanced due diligence policies, procedures and controls to be applied to High Risk Foreign Correspondent Banking Customers.

i. Due Diligence Programs for New Correspondent Accounts

As part of its due diligence program, the Bank should assess the money laundering risks presented by each Foreign Bank, as discussed below. In so doing, the Bank should apply, as appropriate, the due diligence elements for Correspondent Accounts set forth below. The Clearing House recognizes that these elements are not exhaustive. For example, the Bank may apply some of the elements of its enhanced due diligence policies, procedures and controls for Correspondent Accounts to a specific Foreign Correspondent Banking Customer, or apply additional measures uniquely tailored for that Foreign Correspondent Banking Customer.

The Bank's due diligence policies, procedures and controls should include some or all of the following, as appropriate:

- obtaining appropriate documentation on the Foreign Bank, such as a government-issued license, that establishes that the Foreign Bank has been duly organized and is in good standing in its jurisdiction of organization (e.g., license to conduct business);
- obtaining the Foreign Bank's annual report;
- identifying the Key Senior Management of the Foreign Bank;
- reviewing information related to the AML and sanctions compliance programs (including a summary of due diligence policies, procedures and controls) of the Foreign Bank. The review may include, but need not be limited to, a discussion with Key Senior Management of the Foreign Bank;
- determining the Foreign Bank's primary lines of business;
- inquiring into the Foreign Bank's local market reputation through review of media reports or by other means;
- evaluating the Foreign Bank's creditworthiness (where credit is being extended);
- obtaining one or more bank references;
- determining the intended use of the Correspondent Account by the Foreign Bank and the expected activity of the Correspondent Account;
- requesting general information on the Foreign Bank's categories of customers, including such categories as Shell Banks, Offshore Banks and other High Risk Foreign Correspondent Banking Customers;
- determining for any Foreign Bank, the shares of which are not publicly traded, the identity of each Owner[5] of the Foreign Bank;

5 For these purposes, "Owner" means "any person who directly or indirectly owns, controls, or has the power to vote 25% or more of any class of securities of a foreign bank." 31 C.F.R. § 1010.600(j).

» determining the type of and restrictions under the Foreign Bank's license;

» determining whether the Foreign Bank has policies and procedures to comply with the requirements established by U.S. bank regulators with regard to Payable-Through Accounts;

» taking into account information, if available, from U.S. law enforcement agencies or U.S. banking authorities, as appropriate, with respect to the Foreign Bank; and

» documenting steps taken (for example, by preparing a Foreign Correspondent Banking Customer due diligence checklist) prior to the opening of a Correspondent Account for the Foreign Bank.

The Bank's due diligence program should enable it to assess the money laundering risks presented by the Correspondent Account, and to detect and report any known or suspected money laundering activity conducted through or involving the Correspondent Account and to determine, if appropriate, whether a Foreign Correspondent Banking Customer requires enhanced due diligence by the Bank.

ii. Enhanced Due Diligence Programs for New Correspondent Accounts

The Bank should apply its enhanced due diligence policies, procedures and controls to new Correspondent Accounts established for High Risk Foreign Correspondent Banking Customers, which may include some or all of the following, as appropriate:

» determining changes in the structure, charter or license of the Foreign Bank;

» determining the relationship between the Foreign Bank and the government of its home country jurisdiction, including whether the Foreign Bank is a government-owned entity;

» reviewing information relating to the Foreign Bank's AML and sanctions compliance program, including a customized AML questionnaire, or a site visit, if appropriate, to assess the program of the Foreign Bank by Compliance (which can be accomplished by telephone interview if logistics prevent such a site visit), where appropriate;

» reviewing pronouncements of United States governmental agencies and multilateral organizations with regard to the adequacy of bank regulation and supervision and AML and counter-terrorist legislation in the Foreign Bank's home country jurisdiction;

» to the extent reasonable, reviewing publicly available information to determine whether the Foreign Bank has been the subject of a money laundering or other criminal investigation, criminal indictment or conviction, any civil enforcement action based on violations of AML laws or regulations or any investigation, indictment, conviction or civil enforcement action relating to financing of terrorists; and

» meeting with Key Senior Management of the Foreign Bank at its offices or the offices of an Affiliate of the Foreign Bank, as appropriate, to discuss the opening of the Correspondent Account.

Furthermore, as part of the Bank's enhanced due diligence policies, procedures and controls, the Bank must determine, for any Foreign Bank

whose shares are not publicly traded, the identity of each Owner[6] of the Foreign Bank and the nature and extent of the ownership interest of each Owner.

iii. Oversight Approval Responsibility for New Correspondent Accounts for High Risk Foreign Correspondent Banking Customers

The Bank should develop and maintain policies, procedures and controls under which, before opening a Correspondent Account for a High Risk Foreign Correspondent Banking Customer, all such Foreign Banks are approved by a person other than the relationship manager primarily responsible for the establishment of the Foreign Bank's Correspondent Account, which may be an officer senior to the relationship manager in the same department as the relationship manager, or an officer in another department (e.g., the Bank Secrecy Act officer, the risk management department, or compliance department) of the Bank.

iv. Updating Due Diligence on Existing Correspondent Accounts

The Bank should develop and maintain policies, procedures, systems and controls that are reasonably designed to ensure that the Bank periodically reviews, and updates its due diligence on, the Correspondent Account of the Foreign Correspondent Banking Customer. The periodic review should include an update of due diligence information on the customer, a review of current activity in the Correspondent Account against past and anticipated activity, and a recalibration of the Bank's AML or financial crime risk assessment, if appropriate. The updated due diligence information on the Foreign Correspondent Banking Customer should be independently reviewed by appropriate personnel at the Bank to ensure the consistency and completeness of the information.

2. RISK ASSESSMENT OF FOREIGN CORRESPONDENT BANKING CUSTOMERS

a. General

The Bank's general due diligence program should include policies, procedures and processes to assess the risks posed by the Bank's Foreign Correspondent Banking Customers, utilizing consistent, well-documented risk rating methodologies. This should enable the Bank to classify the risk level of its Foreign Correspondent Banking Customer in order to determine whether the entity falls within the Bank's risk tolerance. This should also enable the Bank to calibrate its customer due diligence, the frequency of its periodic reviews of its customer due diligence and its enhanced due diligence, in a manner that is consistent with the Bank's risk assessment of the customer. The Bank should incorporate the risk assessment of its customers into the Bank's suspicious activity monitoring systems, which should enable the Bank's resources to be most appropriately directed at those Foreign Correspondent Banking Customers that pose the most significant money laundering risk to the Bank. The Bank's risk assessment should be updated based on periodic reviews of its Foreign Correspondent Banking Customers, which will allow the Bank to recalibrate its due diligence and monitoring of the Foreign Correspondent Banking Customer, as appropriate.

6 For these purposes, "Owner" means "any person who directly or indirectly owns, controls, or has the power to vote 10% or more of any class of securities of a foreign bank." 31 C.F.R. § 1010.610(b)(3)(ii)(A).

b. Risk Assessment Factors for Foreign Correspondent Banking Customers

The Bank's due diligence program should provide for the risk assessment of Foreign Correspondent Banking Customers, considering all relevant factors, including, as appropriate:

» The ownership and control structure of the Foreign Correspondent Banking Customer (e.g., principals, owners, shareholders, directors, signatories, persons with powers of attorney and agents).

» The size and nature of the Foreign Correspondent Banking Customer's business and the market(s) it serves.

» The structure of the legal entity (e.g., to the extent it is publicly traded on a recognized stock exchange[7] or privately held and whether it issues bearer shares[8] and whether it is a parallel banking organization[9]).

» The type, purpose and activity of the Correspondent Account.

- The types of customers of the Foreign Correspondent Banking Customer, including their geographic locations and whether they operate in high-risk or sanctioned countries.
- The types of transactions, and products and services offered by the Foreign Correspondent Banking Customer to its own customers (such as remote deposit capture).

» Whether the Correspondent Account is being used to provide services to other financial institutions and, if so, the nature of those services and a general description of the financial institutions the Foreign Correspondent Banking Customer is serving, with a focus on the factors relating to the financial institution's AML and sanctions risks.

- Whether the Foreign Correspondent Banking Customer itself retains complete access to the Correspondent Account or whether it gives third parties—including its customers—direct access to the Correspondent Account that is a payable-through account.

» The nature and duration of the Bank's relationship with the Foreign Correspondent Banking Customer (and, if relevant and appropriate, with any affiliate of the Foreign Correspondent Banking Customer).

» The AML, sanctions and supervisory regime of the jurisdiction that issued the charter or license to the Foreign Correspondent Banking Customer.

- The AML, sanctions and supervisory regime of the jurisdiction in which any company that is an owner of the Foreign Correspondent Banking Customer is incorporated or chartered.

» Information known or reasonably available to the Bank about the Foreign Correspondent Banking Customer's AML and sanc-

7 Not all institutions are considered "to be traded on recognized stock exchanges" because not all stock exchanges have a methodology for identification that meets the transparency and disclosure requirements of the United States.

8 If bearer shares are identified in the bank's ownership structure, an assessment should be done to determine the risk of the Foreign Correspondent Banking Customer.

9 If a Bank determines that it is dealing with a parallel banking organization, the Bank should refer to the FFIEC BSA/AML Examination Manual (2010) and the Joint Agency Statement on Parallel-Owned Banking Organizations (Apr. 23, 2002).

tions record, including public information in standard industry guides, periodicals and major publications.

» The adequacy and reasonableness of the Foreign Correspondent Banking Customer's AML and sanctions compliance program. For example: whether the Foreign Correspondent Banking Customer uses an automated or manual AML and sanctions compliance system for screening purposes and gathering KYC information about its customers.

» Any negative news known or reasonably available to the Bank about the Foreign Correspondent Banking Customer.

The above list of risk assessment factors for Correspondent Accounts is not an exhaustive list, and Banks may determine that they need not evaluate all of the above factors for every Correspondent Account.

c. Conclusion

Banks may decide to review their Foreign Correspondent Banking Customers and reassess their risk profiles, depending on a triggering event, such as negative news, subpoenas, law enforcement inquiries, requests for information by the Treasury's Financial Crimes Enforcement Network ("FinCEN") pursuant to Section 314(a) of the PATRIOT Act, requests by other financial institutions under Section 314(b) of the PATRIOT Act, national security letters, regulatory enforcement actions relating to money laundering and sanctions, and multiple filings of suspicious activity reports ("SARs") relating to activity in Correspondent Accounts. As part of its ongoing due diligence, Banks should periodically review their Foreign Correspondent Banking Customers' Correspondent Accounts and determine whether their risk profiles need to be readjusted.

Increases in the risks of a Foreign Correspondent Banking Customer should be escalated, as appropriate, by the Bank (including, where warranted, to its BSA Officer or designee and senior management or general counsel) and dealt with appropriately by the Bank. Any increases in the risk profile of a Foreign Correspondent Banking Customer may cause the Bank to enhance its due diligence and/or monitoring of the Correspondent Account, or prohibit the Correspondent Account from dealing with specific entities involved in suspicious activity and putting those entities into the Bank's screening filters. The Bank may also undertake measures to restrict certain activities of the Correspondent Account, or if the risks become outside the risk tolerance of the Bank, the Bank may decide to terminate the Bank's relationship with the Foreign Correspondent Banking Customer.

3. PROHIBITED RELATIONSHIPS WITH CORRESPONDENT ACCOUNTS

The Bank should implement policies, procedures and controls that prohibit the establishment of Correspondent Accounts for certain foreign financial institutions. See Appendix B for further guidance on certain prohibited correspondent relationships.

a. Foreign Banks Designated by the Secretary of the Treasury as Being of Primary Money Laundering Concern

Under Section 311 of the PATRIOT Act, the Bank may be prohibited from opening, maintaining,

administering or managing in the United States any Correspondent Account or payable-through account for, or on behalf of, a foreign bank if the account involves a jurisdiction, financial institution, class of transactions or type of account that has been designated by the Secretary of the Treasury as being of primary money laundering concern ("Section 311 Designated Entity").

In many cases, Treasury regulations imposing special measures (1) prohibit the Bank from knowingly providing indirect access to a Section 311 Designated Entity through its Foreign Correspondent Banking Customer relationships; (2) require that the Bank notify Foreign Correspondent Banking Customer accountholders that they must not use the Correspondent Account to provide services to the Section 311 Designated Entity; and (3) require that the Bank take reasonable steps to identify any indirect use of its Correspondent Accounts by the Section 311 Designated Entity.[10]

During the pendency of a proposed rule imposing special measures, the Bank should consider any guidance issued by Treasury carefully, and take action, as it deems appropriate, to address the risks disclosed by Treasury in the proposed rule. Specifically, the Bank should consider the risks of continuing to do business with a foreign bank that the Secretary of the Treasury has proposed to designate as being of primary money laundering concern. In addition, the Bank may want to consider incorporating such Section 311 Designated Entities—whether such designations have been finalized or merely proposed by the Secretary of the Treasury—into the Bank's screening filters, to identify transactions involving the Section 311 Designated Entities.

b. Foreign Shell Banks

As further discussed in Annex B, the Bank should implement policies, procedures and controls that prohibit the establishment of Correspondent Accounts for or on behalf of Prohibited Foreign Shell Banks.

c. Foreign Banks that Are Subject to U.S. Sanctions

The Bank should take steps to prohibit the establishment of a Correspondent Account in the United States and abroad for, or on behalf of, a foreign bank that is included on the list of Specially Designated Nationals and Blocked Persons administered by the Office of Foreign Assets Control ("OFAC") of the Treasury ("SDN List") or is the subject of the economic sanctions programs administered by the Treasury ("OFAC Sanctions Programs"). The Bank should also undertake appropriate measures with respect to its Correspondent Accounts, such as the blocking of the property or rejection of transactions and filing the requisite blocking or rejection reports with OFAC, as required by the OFAC Sanctions Programs.[11] Banks should be cognizant of other sanctions regimes that may be applicable to them.

10 There are four other special measures under Section 311 of the PATRIOT Act which require that the Bank (1) maintain records or file reports on certain financial transactions, (2) obtain and retain beneficial ownership information of an account, (3) identify each customer and obtain information about each customer relating to certain payable-through accounts, and (4) identify each customer and obtain information about each customer relating to certain Correspondent Accounts. While these four special measures do not prohibit a Bank from maintaining a Correspondent Account with a Section 311 Designated Entity, the Bank may decide to not engage in any relationship with a foreign bank that has been designated by the Secretary of the Treasury as being of primary money laundering concern.

11 It is noted that while correspondent accounts may not be maintained by U.S. banks for foreign banks in countries subject to sanctions, U.S. banks are permitted to process payments to or from such foreign banks that are authorized by general or specific OFAC license.

4. CONFLICTS OF LAWS

A global bank should decide how to address any conflicts of law among jurisdictions where the global bank operates in the most effective way. Any conflicts-of-law issues should be identified by Bank personnel and, as appropriate, escalated to the Bank's AML and sanctions compliance officer and general counsel.

5. IDENTIFICATION AND REPORTING OF SUSPICIOUS CORRESPONDENT ACCOUNT ACTIVITY

The Bank should develop and maintain policies, procedures and controls for identifying, documenting, monitoring, reporting and referring suspicious Correspondent Account activity. This should include reasonable steps on the part of the Bank to conduct enhanced scrutiny of Correspondent Accounts of High Risk Foreign Correspondent Banking Customers, either as independent policies, procedures and controls or as part of the Bank's existing policies, procedures and controls on the identification, reporting and referral of suspicious activity.

a. General

The Bank shall file a timely SAR with Treasury with respect to any suspicious Correspondent Account transaction relevant to a possible violation of law or regulation. See Appendix D for a summary of the SAR filing requirements.

The Bank's policy on the identification, reporting and referral of suspicious Correspondent Account activity should provide for the timely examination of questionable activity to determine and document the reason for the activity and whether the activity constitutes suspicious Correspondent Account activity. It should also provide for the timely referral of suspicious Correspondent Account activity to appropriate personnel so that appropriate action may be undertaken by the Bank to file a timely SAR with Treasury. Banks should have procedures for escalating, as appropriate to senior management and/or the BSA Officer or designee, significant concerns identified by the filing of a SAR.

b. Activity Review/Monitoring

The Bank should monitor the activity in Correspondent Accounts for Foreign Correspondent Banking Customers, including information in payment messages relating to transactions that the Foreign Correspondent Banking Customers undertake on behalf of their customers, with the objective of identifying, investigating and, where appropriate, reporting suspicious activity. The Bank should incorporate information relating to its risk assessment of Foreign Correspondent Banking Customers, as well as information derived from its due diligence and enhanced due diligence policies, procedures and controls, into the Bank's processes for investigation of suspicious Correspondent Account activity.

In developing appropriate methods of activity review or monitoring, the Bank is encouraged to determine whether automated or manual review is suitable and practical under the circumstances, taking into account the size of its correspondent banking portfolio, the risk profile of its customers, the nature of their activity and the available technology.

As part of its monitoring systems, there is an expectation that the Bank should incorporate the results of its monitoring with its due diligence of

the Foreign Correspondent Banking Customer and reassess the actual activity of the Correspondent Account to determine whether there is anything suspicious to report or a rationale for changing the Bank's risk assessment of the Foreign Correspondent Banking Customer.

The Bank should engage in an enterprise-wide approach to its monitoring and investigation of suspicious Correspondent Account activity. Challenges to an enterprise-wide approach for Banks that have multinational locations may include data privacy laws, confidentiality restrictions and logistical issues for the sharing of information among affiliates of the Bank (see Section 5.4 below for Confidentiality of SARs).

c. Examples of Possible Suspicious Correspondent Account Activity

The suspicious activity in a Correspondent Account may derive from the activity of the Foreign Correspondent Banking Customer itself or the underlying parties to a transaction processed through the Correspondent Account. The Bank's policy on the identification and reporting of suspicious Correspondent Account activity should include examples of the types and patterns of transactions that may require further review to determine whether the activity is suspicious. Such examples should be used to raise awareness and assist Bank personnel in considering whether certain transactions may warrant closer scrutiny. Not all transactions exhibiting some of the characteristics of the example transactions necessarily warrant further investigation. The decision to investigate specific transactions must be based upon the particular facts and circumstances relating to the transactions in question. An illustrative list of possible suspicious Correspondent Account activity can be neither exhaustive nor a substitute for the judgment required to determine whether a particular transaction is suspicious. A list of red flags for possible suspicious Correspondent Activity can be found in Appendix D.

Generally, in the context of Correspondent Account activity, determining whether a transaction is suspicious requires an examination of the available facts, including the background and possible purpose of the transaction. In conducting such an examination, the Bank may request that the Foreign Correspondent Banking Customer provide details regarding the Foreign Correspondent Banking Customer's customers and transactions. A Foreign Correspondent Banking Customer is subject to its local laws which may affect the extent to which it is permitted to provide detailed information in response to inquiries from the Bank, and, in such circumstances, the Bank may need to inform the appropriate banking or law enforcement authorities that it is unable to obtain requested information.

d. Confidentiality of SARs

A SAR, and any information that would reveal the existence of a SAR, is confidential and shall not be disclosed except where requested by FinCEN or any federal, state or local law enforcement agency, or any federal or state regulatory authority that examines the bank for compliance with the Bank Secrecy Act.

The Bank may share its SARs and supporting documentation relating to its Foreign Correspondent Banking Customers with its (1) head office and Controlling Companies, whether the

entity is located in the U.S. or abroad,[12] and (2) affiliates provided that they are subject to a SAR regulation.[13] In each case, the Bank should maintain appropriate controls to protect the confidentiality of SARs.

6. PREVENTING UNWANTED USE OF CORRESPONDENT SERVICES

The Bank may consider implementing policies, procedures and controls that enable it to prevent Foreign Correspondent Banking Customers from using their Correspondent Accounts to provide services to persons or entities, including nested Foreign Banks, that the Bank has decided not to do business with directly. In so doing, the Bank may consider establishing its own AML and sanctions-related private lists of prohibited persons and entities, or persons and entities that the Bank subjects to enhanced monitoring. The Bank may consider including the names of these prohibited persons and entities in its monitoring systems for purposes of screening them against transaction data. The Bank may also consider using its monitoring systems to detect use of its Correspondent Accounts to provide services to those persons and entities.

In the event that the Bank's monitoring systems disclose a potential match to its private lists, the Bank should provide for the referral of those potential matches to appropriate personnel as directed by the Bank's policies and procedures for investigation. If the Bank's investigation concludes that it is a match, then the Bank should follow its normal procedures to determine suitable action, including whether to reject the payment or restrict or close the account, and, if appropriate, file a SAR with Treasury.

7. PAYMENT PROCESSING

a. Increased Transparency for Cross-Border Cover Payments

As indicated in the interagency guidance on "Transparency and Compliance for U.S. Banking Organizations Conducting Cross-Border Funds Transfers," the Basel Committee on Banking Supervision issued a paper entitled "Due diligence and transparency regarding cover payment messages related to cross-border wire transfers" ("BIS Cover Payments Paper") in May 2009, addressing transparency in cross-border cover payment messages. According to the interagency guidance, the BIS Cover Payments Paper encourages increased transparency for cross-border cover payments and it also encourages all banks involved in international payments transactions to adhere to the message standards developed by The Clearing House and the Wolfsberg Group in 2007 ("Message Standards"). To address the risks related to a lack of transparency in the international payments system, the Bank should implement policies, procedures and controls to apply increased transparency for cross-border cover payments and adhere to the Message Standards, as noted in the interagency guidance. 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 process;

12 Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies, issued by the Financial Crimes Enforcement Network, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency and Office of Thrift Supervision (Jan. 20, 2006).

13 Interagency Guidance. See 31 CFR §§ 103.15 to 103.21. See also, 12 CFR § 208.62 (FRB); 12 CFR § 353.3 (FDIC); 12 CFR § 748.1 (NCUA); 12 CFR § 21.11 (OCC); and 12 CFR § 563.180 (OTS).

» 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 Foreign Correspondent Banking Customers to observe these principles.

Consistent with FATF Recommendation 16 and the FFIEC BSA/AML Examination Manual, a Bank should take measures to ensure that financial institutions include required and accurate originator information and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain, in compliance with Treasury regulation, i.e., 31 C.F.R. § 1020.410. A Bank should also monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information (e.g., information is missing, manifestly meaningless or incomplete, or suspicious), and take appropriate steps.

A Bank should ensure that, in the context of its processing of wire transfers for the Correspondent Accounts of its Foreign Correspondent Banking Customers, it takes appropriate action as required by OFAC regulations, including blocking or rejecting wire transfers with countries, persons or entities subject to the OFAC sanctions programs.

b. Monitoring for Use of MT202 When MT202COV Is Required

SWIFT developed a new payment instruction format, i.e., the MT 202 COV, that must be used for any bank-to-bank transfer that is a cover payment for a commercial (MT 103) payment. Information relating to the originator and beneficiary is mandatory in the MT 202 COV. The Bank should strongly encourage its Foreign Correspondent Banking Customers to follow SWIFT standards in this regard. (The discussion noted herein with regard to MT 202 and MT 202 COV also applies to MT 205 and MT 205 COV although the discussion does not separately reference MT 205 and MT 205 COV.)

Intermediary banks are not in a position to determine whether any particular bank-to-bank transfer is a cover payment and therefore they cannot determine whether the use of the MT 202 or MT 202 COV is appropriate under SWIFT standards for any particular payment. However, the Bank should consider factoring into its risk assessment of a Foreign Correspondent Banking Customer any known instance, policy or practice of using the wrong type of message, and should consider having appropriate controls in place if a Foreign Correspondent Banking Customer fails to use the appropriate message format. Where the Bank knows or suspects that a Foreign Correspondent Banking Customer has used the wrong message to avoid detection of information by other financial institutions, the Bank should consider filing a SAR on that particular Foreign Correspondent Banking Customer.

c. Identifying Cancelled and Resubmitted Payments

Where a payment sent through the United States by a Foreign Correspondent Banking

Customer is blocked or rejected by a Bank due to indicia in the payment message that processing the payment may contravene U.S. sanctions laws, and a payment involving the same or similar parties and for the same or a similar amount is later re-sent with the sanctions-related information either amended or omitted, this type of behavior may be indicative of an attempt to conceal information in order to evade the sanctions laws. Accordingly, as part of its monitoring of the activity of a Foreign Correspondent Banking Customer, the Bank may want to consider implementing measures to identify and investigate payments that may represent resubmissions of payments previously blocked or rejected due to sanctions concerns. The Bank should have policies to address instances where such potential resubmissions are identified. These policies may include the undertaking of enhanced monitoring of the Foreign Correspondent Banking Customer that resubmits a payment previously blocked or rejected due to sanctions concerns, including a mandatory review of all payments processed by the Foreign Correspondent Banking Customer through its Correspondent Account for a reasonable period to ensure that no more payments are processed in violation of the U.S. sanctions laws.

8. INTERNATIONAL CASH LETTER AND REMOTE DEPOSIT CAPTURE

a. International Cash Letter

An international cash letter entails the use of a carrier, courier (either independent or common) to transport monetary instruments from outside the United States to a bank in the United States for processing negotiable instruments between banks located in different countries. The cash letter contains a number of negotiable items, normally checks (commercial checks, travelers checks and money orders), accompanied by a deposit ticket listing each item and corresponding dollar amount. Upon receipt from its Foreign Correspondent Bank Customer, the Bank sends the monetary instruments for clearance or negotiation to the financial institution(s) upon which the individual items were originally drawn. The foreign bank's account at the U.S. clearing bank will then be credited for the total amount of the cash letter.

International cash letters received from Foreign Correspondent Banking Customers that are processed through their Correspondent Accounts may expose Banks to various risks, including money laundering, fraud and credit risk associated with return items. Banks should be aware that both U.S. financial institutions and law enforcement have identified bulk amounts of monetary instruments purchased in the United States that appear to have been structured to avoid BSA-reporting requirements in cash letters received from foreign financial institutions, especially from jurisdictions with lax AML controls. Additionally, Banks should be aware that U.S. financial institutions have identified checks received in cash letters that have been endorsed to a third party and presented to banks located overseas, where the drawer and payee appear unconnected to the area where the checks are presented. Such activity may be indicative of money laundering.

i. Risk Assessment of Cash Letters

Legal and Compliance Risks. A Bank should evaluate potential risks and regulatory requirements under BSA laws and regulations associated with the provision of cash letter services to Foreign Correspondent Banking

Customers. The Bank should consider whether and to what extent it could be exposed to the risk of money laundering activities, as well as its ability to comply with AML laws and regulations, including its ability to monitor Foreign Correspondent Banking Customers for suspicious activity relating to their use of cash letter services. A Bank should consider developing and maintaining written policies and procedures governing cash letter services. The Bank's policies should describe acceptable and unacceptable transactions (such as monetary instruments with blank payees, consecutively numbered negotiable instruments or checks endorsed to third parties and presented in a location that does not appear to relate to the drawer or payee).

Customer Due Diligence and Eligibility. A Bank should maintain and adhere to criteria for determining whether to provide cash letter services to a Foreign Correspondent Banking Customer. In general, information gathered while conducting customer identification and customer due diligence procedures in fulfillment of the institution's BSA compliance program can support this assessment. The Bank should also maintain criteria for ceasing to provide cash letter services.

ii. Monitoring for Suspicious Cash Letters

The Bank should consider implementing policies, procedures and processes for the monitoring of cash letter services activities that are reasonably designed to identify suspicious activity and include clearly supported and documented logic for monitoring such activities. Banks should consider developing a list of red flags that would suggest unusual or suspicious activity that is specific to cash letter services.

b. Remote Deposit Capture

i. Generally

The Remote Deposit Capture ("RDC") service offered by a Bank to its Foreign Correspondent Banking Customer is a deposit transaction delivery system, which allows a Foreign Correspondent Banking Customer to scan a check or monetary instrument (e.g., traveler's checks or money orders), and then transmit the scanned or digitized image to the Bank. It essentially allows the Foreign Correspondent Banking Customer to deposit items electronically from remote locations without any face-to-face interaction with the Bank.

The offering of RDC services may expose a Bank through its Foreign Correspondent Banking Customer's Correspondent Account to various risks, including money laundering, fraud and information security risk. The challenges for a Bank to deal with the risks of RDC services are becoming more prevalent as Foreign Correspondent Banking Customers are increasingly using RDC services to replace pouch and certain instrument-processing and clearing activities. Inadequate controls at the Bank could result in intentional or unintentional alterations to deposit item data, resubmission of a data file or duplicate presentment of checks and images at the Bank. In addition, original deposit items are not typically forwarded to the Bank, but instead are retained by the Foreign Correspondent Banking Customer, or the Foreign Correspondent Banking Customer's customer or service provider, increasing recordkeeping, data safety and integrity issues.

This inevitably creates a risk for the Bank—where the Foreign Correspondent Banking Customer's Correspondent Account is maintained and through which the customers' deposits of

the Foreign Correspondent Banking Customer are made—which has minimal visibility into the transaction being effected via the RDC services offered by the Bank to the Foreign Correspondent Banking Customer.

ii. FFIEC Guidance on RDC

Acknowledging the risk factors associated with RDC, the FFIEC Manual recommends that management develop appropriate policies, procedures and processes to mitigate these risks. The Manual provides the following non-exhaustive list of examples of risk mitigants:

- identifying and assessing the risk associated with the RDC activity at the Foreign Correspondent Banking Customer;
- conducting appropriate CDD and EDD on the Foreign Correspondent Banking Customer;
- creating risk-based parameters (e.g., Foreign Correspondent Banking Customer's credit history, financial statements, ownership structure of business, risk management processes, geographic location and customer base) for determining the acceptability of a Foreign Correspondent Banking Customer's RDC activity, and when the level of risk warrants, conducting additional due diligence on the Foreign Correspondent Banking Customer's RDC activity (including visiting the Foreign Correspondent Banking Customer's physical location as part of the suitability review);
- if known, conducting due diligence on the vendor used by the Foreign Correspondent Banking Customer for RDC activities, and ensuring that the Foreign Correspondent Banking Customer has implemented sound vendor management processes;
- obtaining expected account activity from the Foreign Correspondent Banking Customer and comparing it to actual activity and the business type to ensure they are reasonable and consistent;
- establishing and, as appropriate, modifying RDC transaction limits, which are acceptable and unacceptable to the Bank;
- developing well-constructed contracts, which address, among other things, the Foreign Correspondent Banking Customer's responsibility to prevent its customers' inappropriate use of its RDC services and provide original documents on its customers' RDC activity to the Bank in order to facilitate its investigations related to unusual transactions, and the Bank's authority to mandate specific internal controls, conduct audits or terminate the Foreign Correspondent Banking Customer's RDC relationships with its customers;
- implementing additional monitoring or review when significant changes occur at the Foreign Correspondent Banking Customer; and
- ensuring that the Foreign Correspondent Banking Customer receives adequate training in order to address the risks associated with its customers' RDC activity.

iii. Monitoring for Suspicious RDC Activities

The Bank should consider implementing policies, procedures and processes for the monitoring of RDC activities conducted by the Foreign Correspondent Banking Customer through the Correspondent Account maintained at the Bank that are reasonably designed to identify

suspicious activity. This may include the Bank's monitoring of the Foreign Correspondent Banking Customer's rate of return on its RDC activity for purposes of determining whether the RDC activity is suspicious.

9. BULK CASH

a. General

A shipment of bulk cash entails the use of common, independent or Postal Service carriers to transport large volumes of U.S. or non-U.S. bank notes from sources either inside or outside the United States to a Bank that is located in the United States.

A Bank is required to report any physical transportation, mailing or shipment of currency or other monetary instruments in an aggregate amount exceeding $10,000 received from, or shipped to, locations outside the U.S., on a Report of International Transportation of Currency or Monetary Instruments (i.e., CMIR or Form 105). A Bank is exempt from this reporting requirement when the currency or other monetary instruments are mailed or shipped through the Postal Service or common carrier. However, the exemption does not apply to the mailing or shipment of currency or other monetary instruments by other methods, such as air courier or the airlines.

In addition, a Bank is required to report the receipt or disbursement of currency in excess of $10,000 on a Currency Transaction Report (i.e., FinCEN Form 104), subject to certain exemptions. This reporting requirement applies even if the international transactions are subject to the exemption from filing a CMIR or Form 112.

Moreover, a Bank is required to monitor and report suspicious activity relating to shipments of bulk cash. To effectively monitor suspicious shipments of bulk cash, a Bank should establish and implement additional due diligence measures with regard to the Foreign Correspondent Banking Customers that process such shipments through their Correspondent Accounts, as appropriate, depending on the Bank's risk assessment of the Foreign Correspondent Banking Customer.

b. Risk Assessment

Banks should determine the risk that their Foreign Correspondent Banking Customers receive payments relating to bulk shipments of currency in their Correspondent Accounts that could originate from illicit activity. Correspondent Accounts of Foreign Correspondent Banking Customers are particularly susceptible to this risk. Since bulk cash that is smuggled out of the United States is usually denominated in U.S. dollars, those who receive the smuggled bulk cash must find ways to reintegrate the currency into a U.S. Bank.

To guard against this risk, a Bank may want to consider implementing policies, procedures and processes to manage the risks associated with its Foreign Correspondent Banking Customers' receipt of bulk currency shipments from their customer base, which may be composed of Currency Originators (i.e., individuals or businesses that generate currency from cash sales of commodities or other products or services (including monetary instruments or exchanges of currency)) and Intermediaries that ship currency from their customers who are Currency Originators or other Intermediaries. In this regard, a Bank may want to consider implementing a risk

assessment process that considers whether its Foreign Correspondent Banking Customers offer bulk currency services to their customers, and considers the nature, source, location, and control of the bulk currency, and the characteristics of the Foreign Correspondent Banking Customer's customer base.

The results of the Bank's risk assessment should be incorporated into the Bank's customer due diligence and enhanced due diligence procedures. The risk assessment results should also be incorporated into the Bank's monitoring systems for suspicious activity with regard to its Foreign Correspondent Banking Customers.

c. Due Diligence Regarding Bulk Currency Shipments

A Bank should establish and implement additional due diligence measures with regard to the Foreign Correspondent Banking Customers that process payments related to bulk currency shipments through their Correspondent Account, as appropriate, based on the Bank's risk assessment.

These due diligence measures may include: (i) obtaining information about the sources of the bulk cash shipments, including names of Currency Originators and Intermediaries; (ii) a determination of the expected volumes of payments related to bulk cash shipments, frequency of transactions, sources of funds, and reasonableness of volumes based on Originators and Intermediaries; and (iii) the establishment of an agreement or contract with a Foreign Correspondent Banking Customer regarding its AML policies, procedures and processes relating to its bulk cash business.

A Bank should establish a relationship approval process relating to its Foreign Correspondent Banking Customer's processing of bulk cash shipments through its Correspondent Accounts.

d. Monitoring for Suspicious Bulk Currency Shipments

A Bank should closely monitor bulk currency shipment transactions involving its Foreign Correspondent Banking Customers' Correspondent Accounts so that it is able to detect and report suspicious activity, with a particular emphasis on the reasonableness of transaction volumes from Foreign Correspondent Banking Customers on behalf of a customer base.

10. SANCTIONS COMPLIANCE

a. OFAC Risk Assessment

A Bank should implement policies, procedures and processes for assessing the OFAC risks associated with each Foreign Correspondent Banking Customer that maintains a Correspondent Account at the Bank. As part of its risk assessment, the Bank should take into account a composite of applicable factors related to the Foreign Correspondent Banking Customer, including those referred to in Section 2 entitled "Risk of Foreign Correspondent Banking Customers."

In general, information gathered by the Bank on the Foreign Correspondent Banking Customer through its performance of customer identification and customer due diligence procedures in fulfillment of the institution's BSA compliance program can support the

Bank's assessment of the OFAC risks of the Foreign Correspondent Banking Customer. Banks should periodically reassess the OFAC risks posed by Foreign Correspondent Banking Customers. Once the Bank has conducted its OFAC risk assessment of Foreign Correspondent Banking Customers, it should develop appropriate policies, procedures and processes to address such risk.

b. Internal Controls for Sanctions Compliance

i. Monitoring of Correspondent Account Activity for Sanctioned Transactions and Reviewing Such Activity

A Bank should implement policies, procedures and processes to address how the Bank will identify and review Foreign Correspondent Banking Customers and transactions that occur through their Correspondent Accounts for possible violations of U.S. sanctions laws. This can be done either manually or through the use of interdiction software or a combination of both. To determine whether a Foreign Correspondent Banking Customer, or transactions conducted through the Foreign Correspondent Banking Customer's Correspondent Account, violate U.S. sanctions laws, the Bank should screen the names and identifying information of the Foreign Correspondent Banking Customer and parties to the transactions against the list of persons, entities and countries with which the Bank is prohibited from engaging in transactions or providing services, targeted by the OFAC Sanctions Programs, including the SDN List.

The Bank's OFAC compliance program should include policies, procedures and processes for screening Foreign Banks against the SDN List prior to (or shortly thereafter) opening a Correspondent Account for them. The Bank should restrict transactions in the Correspondent Account, with limited exceptions (e.g., initial deposits), until the Bank has conducted the necessary OFAC checks on the new Account. Once the Bank has completed its initial OFAC checks and the Account has been opened, the Bank's OFAC compliance program should also include policies, procedures and processes for checking existing Foreign Correspondent Banking Customers, and the transactions conducted through their Correspondent Accounts at the Bank, against the OFAC Sanctions Programs, including the SDN List, as they are amended from time to time. The frequency of the Bank's review will vary, depending on the Bank's assessment of the OFAC risks associated with the Foreign Correspondent Banking Customer. Transactions effected by the Foreign Correspondent Banking Customer through its Correspondent Account, such as funds transfers and letters of credit, should also be screened for OFAC purposes prior to the execution of such transactions. The Bank should continue to timely update its manual or automated systems with any changes to the SDN List or the list of countries that make up the OFAC Sanctions Programs, as well as licenses, and distribute such information to its domestic and foreign operations so the Bank can continue to check its Foreign Correspondent Banking Customers and transactions that occur through their Correspondent Accounts against the updated SDN List and OFAC Sanctions Programs.

Since the U.S. government has the ability to impose strict conditions on Correspondent Accounts of Foreign Banks based on activities delineated under certain U.S. sanctions laws, such as the Iran Sanctions Act of 1996, the Comprehensive Iran Sanctions, Accountability, and

Divestment Act of 2010, the National Defense Authorization Act for Fiscal Year 2012 and the Iran Freedom Counter-Proliferation Act of 2012, a Bank may want to consider implementing policies, procedures and processes, as appropriate, to address these issues. This may include enhancements to the Bank's customer due diligence procedures, which will enable the Bank to detect whether a Foreign Correspondent Banking Customer is engaging in sanctionable activities.

A Bank may share information about parties, or the transactions in which they engage, targeted by U.S. sanctions laws, with other financial institutions pursuant to Section 314(b) of the PATRIOT Act and its implementing regulation, i.e., 31 C.F.R. § 1010.540, which is discussed in greater detail in Appendix C.

In the event that a Bank outsources to a third-party vendor or service provider, the responsibility of conducting OFAC checks of Correspondent Accounts on its behalf, the Bank still remains ultimately responsible for its compliance with U.S. sanctions laws with regard to such Accounts. Therefore, the Bank should consider establishing adequate controls and review procedures for such relationships.

The Bank should implement policies, procedures and processes relating to its review of the potential hits arising out of its OFAC checks, as noted above. Based on its review, the Bank may take one of the following actions: (1) it may decide to close out the potential hit as a false positive, in which case it should document its reasons for closing out the hit, or (2) in the event it finds that it is a valid match, the Bank should escalate the match for further review to the compliance or legal area, which will, in turn, determine the appropriate action the Bank should undertake with respect to such match.

The Bank's development of a robust OFAC compliance program is significant for two reasons: first, such a program will help to protect the Bank from potential violations of the strict liability regime of U.S. sanctions laws; and second, in the event there is a violation of U.S. sanctions laws by the Bank, the adequacy of the Bank's OFAC compliance program (which includes the Bank's ability to cease its continued operation of a Correspondent Account or processing of transactions in such Account post-designation) will be considered a mitigating factor in OFAC's determination of penalty actions against the Bank for such violations pursuant to OFAC's "Economic Sanctions Enforcement Guidelines."

ii. OFAC Regulations: Rejecting Transactions or Blocking Property and Filing Reports with OFAC

Once the Bank has determined that it has a valid match from its OFAC checks, as described above, the Bank's OFAC compliance program should include policies, procedures and processes for complying with OFAC regulations, including the rejection of the transaction or blocking of property and filing of reports with OFAC. You should refer to Appendix E for additional information on these OFAC regulations.

iii. FinCEN Guidance on Filing SARs on OFAC-Sanctioned Activities

Pursuant to FinCEN's interpretive guidance, a Bank no longer is required to file a SAR on property blocked by the Bank, provided it has filed a blocked property report with OFAC, unless the SAR contains information not included in the blocked property report filed with OFAC. Refer to Appendix E for additional information on the guidance.

11. THE COMPREHENSIVE IRAN SANCTIONS, ACCOUNTABILITY, AND DIVESTMENT ACT OF 2010 ("CISADA") AND THE IRAN FINANCIAL SANCTIONS REGULATIONS

a. Section 104(e) of CISADA

i. General Requirements

Pursuant to Section 104(e) of CISADA and its implementing regulation, i.e., 31 C.F.R. § 1060.300, the Bank may want to consider implementing policies, procedures and controls for responding to written requests from FinCEN regarding specified Foreign Banks. Such procedures may include steps to request its Foreign Correspondent Banking Customers to certify:

- Whether it maintains a Correspondent Account for an Iranian-linked financial institution designated under the International Emergency Economic Powers Act ("IEEPA");
- Whether it has processed any funds transfer within the preceding 90 calendar days for or on behalf of, directly or indirectly, an Iranian-linked financial institution designated under IEEPA, other than through a Correspondent Account; and
- Whether it has processed any funds transfer within the preceding 90 calendar days for or on behalf of, directly or indirectly, IRGC-linked persons designated under IEEPA.

The Bank should request that the Foreign Correspondent Banking Customer agree to notify it if the Foreign Correspondent Banking Customer subsequently establishes a new Correspondent Account for an Iranian-linked financial institution designated under IEEPA at any time within 365-calendar days from the date of the Foreign Correspondent Banking Customer's initial response.

ii. Model Certification

FinCEN has published a model certification format, which the Bank may provide to a specified Foreign Correspondent Banking Customer for purposes of documenting its certifications and related information.

iii. Filing Procedures

Upon receiving a written request from FinCEN, the Bank should refer to Treasury's regulations, i.e., 31 C.F.R. § 1060.300, for the information it is required to report to FinCEN regarding the specified Foreign Correspondent Banking Customer. The Bank should also refer to these regulations for the deadlines for filing such reports with FinCEN and the recordkeeping requirements relating to such reports and supporting documents.

12. INFORMATION SHARING

For information on the requirements for information sharing between a Bank and a government agency, or voluntary information sharing between a Bank and other financial institutions, under Sections 314(a) and (b) of the PATRIOT Act, and its implementing regulations (31 C.F.R. §§ 1010.520 and 1010.540), please refer to Appendix C.

13. GOVERNMENT REQUESTS FOR INFORMATION

For information on requests by an appropriate federal banking regulator for a Bank's records pursuant to the "120 Hour Rule" or government requests for information from a Bank (31 U.S.C. §5318(k)(2) and (3)), please refer to Appendix C.

14. INDEPENDENT TESTING

As part of its BSA compliance program, the Bank should develop an independent review process conducted by the Bank's compliance department, internal audit department or an outside firm of independent auditors that have knowledge of or specialize in the area of correspondent banking to review the effectiveness of the Bank's AML policies, procedures and controls in correspondent banking on a periodic basis.

The Bank should report the results of such self-assessment or evaluation to the audit committee of the board of directors of the Bank or similar oversight body.

15. TRAINING

As part of its BSA compliance program, the Bank should provide anti-money laundering training programs that focus on correspondent banking on a periodic basis. The Bank's AML training programs should specifically address correspondent banking, either as part of the general program, or through a program tailored for those employees of the Bank involved in the Bank's correspondent banking business. The Bank should develop and maintain policies, procedures and controls that are reasonably designed to ensure that all relationship managers and other personnel associated with its correspondent banking unit attend the AML training programs. The training programs should, among other things, review:

» applicable AML laws and recent trends in money laundering, including the ways in which such laws and trends relate to correspondent banking; and

» the Bank's own policies, procedures and controls to combat money laundering, including how to identify and report suspicious Correspondent Account activity.

Appendix A

Definitions

Unless otherwise defined, capitalized terms used in the Guiding Principles have the meanings set forth below:

"Affiliate" means any Foreign Bank that is controlled by, or is under common control with, a depository institution, credit union or Foreign Bank.

"Bank" means any U.S. Bank, or any other financial institution. A "Bank" includes "[e]ach agent, agency, branch or office within the United States of any person doing business in one or more of the capacities listed below: (1) a commercial bank or trust company organized under the laws of any State or of the United States; (2) a private bank; (3) a savings and loan association or a building and loan association organized under the laws of any State or of the United States; (4) an insured institution as defined in section 401 of the National Housing Act; (5) a savings bank, industrial bank or other thrift institution; (6) a credit union organized under the law of any State or of the United States; (7) any other organization (except a money services business) chartered under the banking laws of any state and subject to the supervision of the bank supervisory authorities of a State; (8) a bank organized under foreign law; or (9) any national banking association or corporation acting under the provisions of section 25(a) of the Act of Dec. 23, 1913, as added by the Act of Dec. 24, 1919, ch. 18, 41 Stat. 378, as amended (12 U.S.C. 611-32)." 31 C.F.R. § 1010.100(d).

"Bearer Shares" means unlisted or unregistered share ownership which can be transferred by the physical delivery of the share certificate without any other action. Use of bearer shares allows ownership of a corporation to be conveyed by simply transferring physical possession of share certificates.

"Certification" means a written certificate issued by a Foreign Correspondent Banking Customer, signed by a duly authorized representative of the Foreign Correspondent Banking Customer. A "Recertification" means a written certificate, required of a Foreign Correspondent Banking Customer every three years if the relationship is ongoing, or at any time the Bank has reason to believe the information is no longer accurate.

"Controlling Company" includes a bank holding company ("BHC"), as defined in section 2 of the BHC Act; a savings and loan holding company, as defined in section 10(a) of the Home Owners' Loan Act; and a company having the power, directly or indirectly, to direct the management policies of an industrial loan company or a parent company or to vote 25% or more of any class of voting shares of an industrial loan company or parent company.

"Correspondent Account" means an account established by a Bank for a Foreign Correspondent Banking Customer to receive deposits from, or to make payments or other disbursements on behalf of, the Foreign Correspondent Banking Customer, or to handle other financial transactions related to such Foreign Correspondent Banking Customer. For purposes of this definition, the term "account" means any formal banking or business relationship established by a Bank to provide regular services, dealings and other financial transactions. It includes a demand deposit, savings deposit, or other transaction or asset account and a credit account or other extension of credit. 31 C.F.R. § 1010.605(c).

"Foreign Bank" means a bank organized under foreign law, or an agency, branch or office located outside the United States of a bank. This does not include an agent, agency, branch or office within the United States of a bank organized under foreign law. 31 C.F.R. § 1010.100(u).

"Foreign Financial Institution" means a Foreign Bank. 31 C.F.R. § 1010.605(f)(1)(i).

"High-Risk Foreign Correspondent Banking Customer" means (A) a Foreign Correspondent Banking Customer that is subject to enhanced due diligence under Section 312 of the PATRIOT Act and its implementing regulation, which includes a bank that operates under (i) an offshore banking license; (ii) a banking license issued by a foreign country that has been designated as a Non-Cooperative Jurisdiction; or (iii) a banking license issued by a foreign country that has been designated by the Secretary of the Treasury under Section 311 of the PATRIOT Act (31 U.S.C. § 5318A) as warranting special measures due to money laundering concerns; or (B) any other Foreign Correspondent Banking Customer identified by the Bank as high risk for money laundering. 31 C.F.R. § 1010.610(b)-(c).

An "Iranian-linked financial institution designated under IEEPA" means a financial institution designated by the U.S. government pursuant to IEEPA (or listed in an annex to an Executive order issued pursuant to such Act) in connection with Iran's proliferation of weapons of mass destruction or delivery systems for weapons of mass destruction, or in connection with Iran's support for international terrorism. 31 C.F.R. § 1060.300(a)(2). The list of blocked Iranian-linked financial institutions designated under IEEPA can be found on the list of Specially Designated Nationals and Blocked Persons ("SDN List") administered by Treasury's Office of Foreign Assets Control ("OFAC") at http://www.treasury.gov/ofac/downloads/t11sdn.pdf and followed by the tag [IFSR].

An "IRGC-linked person designated under IEEPA" means Iran's Islamic Revolutionary Guard Corps or any of its agents or affiliates designated by the U.S. government pursuant to IEEPA (or listed in an annex to an Executive order issued pursuant to such Act). 31 C.F.R. § 1060.300(a)(2). The list of blocked IRGC-linked persons designated under IEEPA can be found on OFAC's SDN List at http://www.treasury.gov/ofac/downloads/t11sdn.pdf and followed by the tag [IRGC].

"Key Senior Management" means any person who is a member of the board of directors of a Foreign Bank, excluding an advisory director, or any person who participates or has the authority to participate (other than in the capacity of a member of the board of directors) in major policy making functions of a Foreign Bank.

"Knowledge" means actual knowledge. "Knows" has a corresponding meaning. U.C.C. § 1-202(b). The terms "knows, suspects, or has reason to suspect" mean actual knowledge, or based on all the facts and circumstances, is known to the person, or the person has reason to know or suspect that it exists. This would include a person within the organization who is responsible for an account or transaction coming into possession of facts sufficient to generate a suspicion.

"Non-Cooperative Jurisdiction" means any foreign country that has been designated as non-cooperative with international AML principles or procedures by an intergovernmental group or organization, such as the Financial Action Task Force, of which the United States is a member, and with which designation the United States representative to the group or organiza-

tion continues to concur. Presently there are no Non-Cooperative Jurisdictions.

"Offshore Bank" means any Foreign Bank that possesses a license to conduct banking activities that prohibits the licensing entity from conducting banking activities with the citizens of, or in the local currency of, the jurisdiction that issued the license. 31 C.F.R. § 1010.605(i).

"Payable-Through Account" means a Correspondent Account maintained by a U.S. Bank for a Foreign Bank by means of which the Foreign Bank permits its customers to engage, either directly or through a subaccount, in banking activities usually in connection with the business of banking in the United States. 31 C.F.R. § 1010.610(b)(iii)(B).

"Person" means any individual, corporation, partnership, trust or estate, joint stock company, association, syndicate, joint venture or other unincorporated organization or group; an Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act); and all entities cognizable as legal personalities. 31 C.F.R. § 1010.100(mm).

"Physical Presence" means a place of business that (1) is maintained by a Foreign Bank; (2) is located at a fixed address (other than solely an electronic address or a post-office box) in a country in which the Foreign Bank is authorized to conduct banking activities, at which location the Foreign Bank (i) employs one or more individuals on a full-time basis and (ii) maintains operating records related to its banking activities; and (3) is subject to inspection by the banking authority which licensed the Foreign Bank to conduct banking activities. 31 C.F.R. § 1010.605(l).

"Regulated Affiliate" means a Foreign Shell Bank that (i) is an Affiliate of a depository institution, credit union or Foreign Bank that maintains a Physical Presence in the United States or a foreign country, as applicable; and (ii) is subject to supervision by a banking authority in such country regulating such affiliated depository institution, credit union or Foreign Bank. 31 C.F.R. § 1010.605(n).

"Foreign Correspondent Banking Customer" means any Foreign Bank for which a Bank establishes, maintains, administers or manages a Correspondent Account.

"Prohibited Foreign Shell Bank" is a Foreign Shell Bank that is not a Regulated Affiliate. 31 C.F.R. § 1010.605(g) and (n).

"Foreign Shell Bank" means a Foreign Bank that does not have a Physical Presence in any country. 31 C.F.R. § 1010.605(g).

"U.S. person" means any "person other than an individual (such as a corporation, partnership or trust), that is established or organized under the laws of a State or the United States." 31 C.F.R. § 1010.100(iii).

"United States" means the "States of the United States, the District of Columbia, the Indian lands (as that term is defined in the Indian Gaming Regulatory Act), and the Territories and Insular Possessions of the United States." 31 C.F.R. § 1010.100(hhh).

The "Territories and Insular Possessions of the United States" means the "Commonwealth of Puerto Rico, the United States Virgin Islands, Guam, the Commonwealth of the Northern Mariana Islands, and all other territories and possessions of the United States other than the Indian lands and the District of Columbia." 31 C.F.R. § 1010.100(zz).

Appendix B

Prohibited Relationships with Correspondent Accounts for or on Behalf of Foreign Shell Banks

The Bank should implement policies, procedures and controls that prohibit the establishment of Correspondent Accounts for or on behalf of Prohibited Foreign Shell Banks, as noted below.

Pursuant to Section 313 of the PATRIOT Act, and its implementing regulation, i.e., 31 C.F.R. § 1010.630(a)(1), the Bank should not establish, maintain, administer or manage a Correspondent Account in the United States for, or on behalf of, a Prohibited Foreign Shell Bank. The Bank should also take reasonable steps to ensure that its Foreign Correspondent Banking Customers do not use their Correspondent Accounts to provide banking services to Prohibited Foreign Shell Banks.

To comply with this statute and regulation, the Bank should obtain a Certification from each Foreign Bank seeking to establish a Correspondent Account with a Bank and any Foreign Correspondent Banking Customer with an existing Correspondent Account, certifying (i) that (x) the Foreign Correspondent Banking Customer has a Physical Presence, (y) the Foreign Correspondent Banking Customer does not have a Physical Presence but is a Regulated Affiliate, or (z) the Foreign Correspondent Banking Customer neither has a Physical Presence nor is a Regulated Affiliate; and (ii) that the Foreign Correspondent Banking Customer does not provide banking services to Foreign Shell Banks, or, if the Foreign Correspondent Banking Customer provides banking services to Foreign Shell Banks, it will not use its Correspondent Account to provide banking services to Foreign Shell Banks.

Pursuant to Section 319 of the PATRIOT Act, and its implementing regulation, i.e., 31 C.F.R. § 1010.630(a)(2), the Certification should also request from each Foreign Bank seeking to establish a Correspondent Account with a Bank and any Foreign Correspondent Banking Customer with an existing Correspondent Account, records identifying:

» the Owners[14] of each Foreign Correspondent Banking Customer whose shares are not publicly traded on an exchange or an organized over-the-counter market that is regulated by a foreign securities authority as defined in section 3(a)(50) of the Securities Exchange Act of 1934 (this ownership information is not required to be provided for a Foreign Correspondent Banking Customer that files its ownership information on Form FR Y-7 with the Federal Reserve); and

14 For these purposes, "Owner" means a Person that, directly or indirectly, (i) owns, controls or has power to vote 25% or more of any class of voting securities or other voting interests of a Foreign Correspondent Banking Customer; or (ii) controls in any manner the election of a majority of the directors (or individuals exercising similar functions) of a Foreign Correspondent Banking Customer. For purposes of this definition, members of the same family shall be considered to be one person (and the term same family means parents, spouses, children, siblings, uncles, aunts, grandparents, grandchildren, first cousins, stepchildren, stepsiblings, parents-in-law and spouses of any of the foregoing); and "voting securities or other voting interests" means securities or other interests that entitle the holder to vote for or to select directors (or individuals exercising similar functions). 31 C.F.R. § 1010.605(j).

» the name and address of a person who resides in the United States and is authorized, and has agreed, to be an agent to accept service of legal process from the Secretary of the Treasury or the Attorney General of the United States for records regarding the Correspondent Account maintained on behalf of such Foreign Correspondent Banking Customer.

Pursuant to 31 C.F.R. § 1010.630(b), the Bank will be "deemed to be in compliance" with the statute and regulation if it obtains a Certification from any Foreign Correspondent Banking Customer that maintains a Correspondent Account with the Bank within 30 calendar days after the date the account is established, and a Recertification from such Foreign Correspondent Banking Customer at least once every three years thereafter if the relationship is ongoing or at any time the Bank has reason to believe the information is no longer accurate. The Certification and Recertification forms may be found on the FinCEN website. The Bank may also obtain a Certification or Recertification from the Foreign Correspondent Banking Customer's website, if available.

Appendix C

Information Sharing

1. INFORMATION SHARING BETWEEN A BANK AND GOVERNMENT AGENCY

a. General

Pursuant to Section 314(a) of the PATRIOT Act, and its implementing regulation, i.e., 31 C.F.R. § 1010.520, a federal, state, local or in certain cases, foreign law enforcement agency with criminal investigative authority, investigating terrorist activity or money laundering may request that FinCEN solicit on its own behalf and on behalf of the Treasury Department, or on the investigating agency's behalf, certain information from a Bank, including whether the Bank maintains or has maintained a Correspondent Account for a Foreign Correspondent Banking Customer or has engaged in a transaction with any specified individual, entity or organization in relation to the Correspondent Account of a Foreign Correspondent Banking Customer.

The Bank may want to consider implementing policies, procedures and processes which provide the Bank with steps to follow in order to comply with a FinCEN request for information under section 314(a).

b. A Bank's Search for Records

Using the biweekly report published on the FinCEN website, a Bank should search its records through automated or manual means as applicable, to determine whether the Bank maintains or has maintained a Correspondent Account for a Foreign Correspondent Banking Customer, or has engaged in a transaction with, any specified individual, entity or organization in relation to the Correspondent Account of a Foreign Correspondent Banking Customer which is named in the information request published by FinCEN. A Bank may contact the law enforcement agency named in the FinCEN information request with any questions relating to the scope or terms of the request.

Pursuant to regulations implementing section 314(a), except as otherwise provided in the information request, a Bank should search its records for:

- Any current Correspondent Account maintained for a named suspect;
- Any Correspondent Account maintained for a named suspect during the preceding 12-months; and
- Any transaction conducted by or on behalf of a named suspect, or any transmittal of funds conducted in which a named suspect was either the transmittor or the recipient during the preceding six months, that is required under law or regulation to be recorded by the Bank or is recorded and maintained electronically by the institution.

In its guidance, the Treasury Department narrowed the scope of records through which a Bank must search pursuant to a Section 314(a) request. Unless noted otherwise in the instructions to a section 314(a) request, a Bank is required to conduct a one-time search of the following records for the section 314(a) information:

1. deposit account records (e.g., DDA, checking/share drafts, savings and certificates of deposit);

2. funds transfer records maintained pursuant to 31 C.F.R. § 1010.410;

3. records of the sale of monetary instruments (e.g., cashier's checks, money orders or traveler's checks) maintained pursuant to 31 C.F.R. § 103.29;

4. loan records;

5. trust department account records;

6. records of accounts to purchase, sell, lend, hold or maintain custody of securities;

7. commodity futures, options or other derivatives account records; and

8. safe deposit box records (only if such safe deposit box records are searchable electronically).

Any of the records described above which is not maintained in electronic form need only be searched by a Bank if it is required to maintain such records under federal law or regulation.

A Bank may contract with a third-party service provider or vendor located in the U.S. to search for the requested information. In such a case, the Bank should take steps to safeguard the confidentiality of the information shared with the third party through the use of an agreement or the establishment of adequate procedures to ensure that the third party protect the security and confidentiality of requests from FinCEN for information.

If a Bank identifies a Correspondent Account or transaction with any individual, entity or organization named in the request from FinCEN, the Bank must report it to FinCEN within 14-calendar days unless otherwise specified in FinCEN's request.

c. Use and Confidentiality of the Information Requested

A Bank's use of information provided by FinCEN pursuant to section 314(a) is restricted, in that the Bank may use the information for no purpose other than to:

» report matching information to FinCEN;

» determine whether to establish or maintain a Correspondent Account or engage in a transaction; or

» assist the Bank with its BSA compliance, as required in 31 C.F.R. Part X.

A Bank is prohibited from disclosing to any person—other than FinCEN or the requesting Treasury component, or the law enforcement agency on whose behalf FinCEN is requesting information or U.S. law enforcement attaché in the case of a foreign law enforcement agency—the fact that FinCEN has requested or has obtained information pursuant to such an information request, except to the extent necessary to comply with such an information request. Therefore, a Bank may disclose section 314(a) information to a third-party service provider or vendor located in the U.S. with which it has contracted to search for the requested information so as to enable the Bank to comply with the FinCEN section 314(a) request, provided the Bank takes the necessary steps to ensure that the third-party safeguards the information.

However, the confidentiality provisions of the rule prohibit a Bank from sharing section 314(a) information with any foreign office, branch or affiliate of the Bank (unless the request specifically states otherwise), or affiliates or subsidiaries of bank holding companies to the extent they are not financial institutions as defined under 31 U.S.C. §§ 5312(a)(2) and (c)(1).

Thus, a Bank may want to consider implementing policies, procedures and controls to protect the security and confidentiality of FinCEN requests for information pursuant to section 314(a).

2. INFORMATION AMONG BANKS AND OTHER FINANCIAL INSTITUTIONS

a. General

Pursuant to Section 314(b) of the PATRIOT Act and its implementing regulation, i.e., 31 C.F.R. § 1010.540, a Bank may—under the protection of "safe harbor"—share information with another financial institution or association of financial institutions regarding a Foreign Correspondent Banking Customer, or any individuals, entities, organizations and countries associated with the Foreign Correspondent Banking Customer (including information related to the specified unlawful activities ("SUAs") listed in the U.S. Money Laundering Control Act of 1986 (i.e., 18 U.S.C. §§ 1956 and 1957)), for purposes of identifying and, where appropriate, reporting activities that the Bank suspects may involve possible terrorist activity or money laundering.

To avail itself of the safe harbor from liability protections under section 314(b), a Bank must comply with the notice and use, security and confidentiality of the information requirements, provided below. Accordingly, a Bank may want to consider implementing policies, procedures and controls that provide the Bank with steps it should undertake when seeking to voluntarily share information with another financial institution under the protection of a safe harbor in compliance with the requirements provided under section 314(b) described below.

b. Notice Requirement and Verification

A Bank should submit a notice with FinCEN before sharing any information with another financial institution under section 314(b). The Bank should submit a notice annually if it decides that it wants to continue to share information with financial institutions. The safe harbor protections afforded by the regulation may be lost if the required filing is not made timely.

The Bank should also take reasonable steps to verify that the other financial institution with which the Bank intends to share information has also submitted the required notice to FinCEN, by confirming that the other financial institution appears on a list that FinCEN will periodically make available to financial institutions, generally on the FinCEN website, that the other financial institution has filed a notice with FinCEN or by confirming directly with the other financial institution that the requisite notice has been filed.

c. Use and Security of the Information

Information received by the Bank through such a sharing arrangement with another financial

institution pursuant to section 314(b) may not be used for any purpose other than:

» to identify and, where appropriate, report on money laundering or terrorist activities;

» to determine whether to establish or maintain a Correspondent Account, or to engage in a transaction; or

» to assist the Bank in complying with any requirement of 31 C.F.R. Part X.

The Bank should take steps to implement adequate procedures to safeguard the security and confidentiality of the information shared among the financial institutions.

Section 314(b) does not extend to sharing of information across international borders. In addition, section 314(b) does not permit a Bank to share a SAR, or disclose the existence or non-existence of a SAR. In the event a Bank shares information under section 314(b) about the subject of a SAR, the information shared should be limited to the underlying transaction and the customer information. A Bank may use information obtained under section 314(b) to determine whether to file a SAR. However, the Bank may not share its intention to prepare or file a SAR with another financial institution.

d. Obligation to File a SAR Related to Information Sharing

If, as a result of information sharing with another financial institution under section 314(b), the Bank knows, suspects, or has reason to suspect that an individual, entity or organization is involved in, or may be involved in terrorist activity or money laundering, the Bank should file a SAR in accordance with applicable regulations.

i. Government Requests for Information

Upon request by an appropriate federal banking regulator, a Bank must provide or make available records related to the AML compliance of the Bank or related to one of its Foreign Correspondent Banking Customers within 120 hours from the time of the request. This is otherwise referred to by the banks and government as the "120 Hour Rule."

Also, upon receipt of a written request from a federal law enforcement officer for information maintained by the Bank pertaining to owners of the Foreign Correspondent Banking Customer and the name and address of the person who resides in the United States and is authorized to accept service of legal process for records regarding the Foreign Correspondent Banking Customer's Correspondent Account, the Bank shall provide the information to the requesting officer not later than seven days after receipt of the request.

Appendix D

Suspicious Activity Reporting Requirements

The Bank is required to file a SAR with Treasury with regard to any Correspondent Account transaction that is conducted or attempted by, at or through the Bank (or its affiliate), and it involves or aggregates funds or other assets of at least $5,000, and the Bank "knows, suspects, or has reason to suspect" that:

» the transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;

» the transaction is designed to evade any AML requirements or any other regulations promulgated under the BSA; or

» the transaction has no business or apparent lawful purpose or is not the sort in which the particular Foreign Correspondent Banking Customer would normally be expected to engage, and the Bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

The Bank is also required to file a timely SAR with respect to (i) criminal violations involving insider abuse in any amount, (ii) criminal violations aggregating $5,000 or more when a suspect can be identified, or (iii) criminal violations aggregating $25,000 or more regardless of a potential suspect.

1. RED FLAGS FOR SUSPICIOUS CORRESPONDENT ACCOUNT ACTIVITY

In some circumstances, the following activities, none of which per se constitutes suspicious Correspondent Account activity, may be indicative of Correspondent Account activity that may require further investigation and a closer review:

» the provision of insufficient or suspicious information during the onboarding process;

» the reluctance to provide complete information about the nature and purpose of its account, anticipated account activity, prior correspondent banking relationships, the names of its officers and directors, or information on its business location;

» the activity of a Correspondent Account that is inconsistent with the Foreign Correspondent Banking Customer's business;

» the effectuation of many funds transfers in large, round-dollar, hundred-dollar or thousand-dollar amounts, where the Correspondent Account has not previously been used for similar transfers;

» an unusually large number of funds transfers or fluctuations in the volume of funds transfers;

- transactions effected in bursts of activity within a short period of time;
- funds transfer activity to or from a Correspondent Account that is unexplained, repetitive or shows unusual patterns;
- the engagement in an unusual volume of the Foreign Correspondent Banking Customer's own bank check or dollar draft activity;
- unusually high numbers of returned or rejected items involving a Correspondent Account;
- a request to establish a relationship with, or route a transaction through, a financial institution that is not accustomed to doing business with Foreign Banks and that has not sought out business of that type;
- the routing of transactions through several jurisdictions or financial institutions prior to, or following entry into, the Bank without any apparent purpose other than to disguise the nature, source, ownership or control of the funds;
- the effectuation of frequent or numerous funds transfers originating from or for the benefit of Shell Banks or High Risk Foreign Correspondent Banking Customers;
- fund transfer activity occurring to or from a Correspondent Account originating from or going to a financial secrecy haven or a higher-risk geographic location (such as a Non-Cooperative Jurisdiction) without an apparent business reason, or when the activity is inconsistent with the Foreign Correspondent Banking Customer's business or history;
- beneficiaries of Foreign Correspondent Banking Customers maintaining accounts at Foreign Banks that have been the subject of previous SAR filings due to suspicious wire or other wholesale product activity;
- the reappearance of a beneficiary's banks based in offshore locations, the account of at least one of which has been closed by the Foreign Correspondent Banking Customer due to overall suspect activity;
- large currency or bearer instrument transactions either into or out of the Correspondent Account;
- the deposit or withdrawal from a Correspondent Account of multiple monetary instruments (e.g., traveler's checks, money orders and bank drafts) just below the reporting threshold on or around the same day, particularly if the instruments are sequentially numbered;
- the deposit of U.S. postal money orders in a cash letter coming from a Foreign Correspondent Banking Customer;
- the issuance of large volumes of cashier's checks or bank drafts against the Correspondent Account, particularly when the face amounts are less than local reporting requirements;
- high-value deposits or withdrawals, particularly irregular deposits or withdrawals, not commensurate with the type of Correspondent Account or business of the Foreign Correspondent Banking Customer;
- transactional activity that appears unusual in the context of the relationship with the Correspondent Account;

» funds transfers to or from the Correspondent Account originating from or going to accounts of individuals or entities identified by law enforcement agencies as being suspected of engaging in money laundering or terrorist activities; and

» an inquiry by or on behalf of a Foreign Correspondent Banking Customer regarding exceptions to the reporting requirements of the Bank Secrecy Act (for example, currency transaction reports and SARs) or other rules requiring the reporting of suspicious transactions.

Appendix E

OFAC Regulations: Rejecting Transactions or Blocking Property and Filing Reports with OFAC

Once the Bank has determined that it has a valid match from its OFAC checks, the Bank's OFAC compliance program should include policies, procedures and processes for the Bank to determine whether it should (1) reject the transaction as required by the relevant OFAC regulation, or (2) block the property of the Correspondent Account involved in the transaction and establish an interest-bearing account to hold the blocked property in compliance with OFAC regulations. Additionally, the Bank's policies, procedures and processes should address the OFAC requirement that it file a report with OFAC within 10 business days of rejecting the transaction or blocking the property, and an annual report on the blocked property held by the Bank as of June 30 of each year filed by September 30 of that same year. The Bank's policies, procedures and processes should also address certain instances involving narcotics trafficking or terrorism, when the Bank may want to immediately notify OFAC by phone or e-hotline in addition to filing the requisite reports with OFAC.

1. FINCEN GUIDANCE ON FILING SARS ON OFAC SANCTIONED ACTIVITIES

Pursuant to FinCEN's interpretive guidance, a Bank no longer is required to file a SAR on property blocked by the Bank, provided it has filed a blocked property report with OFAC. However, under the guidance, the Bank's policies, procedures and processes should address instances in which it is in possession of information not included on the blocked property report filed with OFAC, in which case the Bank should file a SAR with FinCEN, containing the additional information. Additionally, the Bank's policies, procedures and processes should consider filing a SAR if the transaction itself would be considered suspicious in the absence of a valid OFAC match in compliance with the suspicious activity reporting rules.