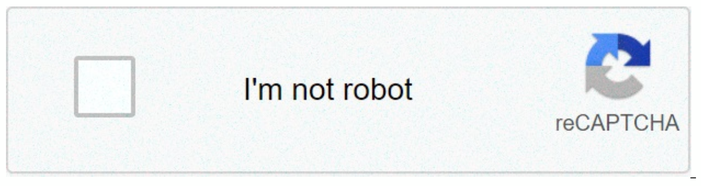

Continue

Currency transaction report exemptions

Goal. Assess the bank's compliance with regulatory and regulatory requirements for exemption from monetary transaction reporting requirements. 1. Determine whether the bank uses the monetary transaction reporting (CTR) exemption process. If so, determine if CTR waiver policies, procedures, and procedures are complete. Phase I exemption (31 CFR 1020.315(b)(1)-(5)) 2. Determine if the bank submits an Electronic Tax Exempt Person Identification report through FinCEN's Electronic Filing System to exempt eligible listed public companies and their subsidiaries from CTR reporting as defined in 31 CFR 1020311. The report must be filed within 30 days from the date the first report transaction is waived. 3. Assess whether an ongoing and reasonable due diligence is carried out, including the annual assessments necessary to determine whether a public company or listed subsidiary is eligible to be identified as an exempt person in accordance with the specified requirements. Management should properly record exemption decisions (e.g., with stock prices from the press and combined profits for the business). Phase II exemption (31 CFR 1020.315(b) (6)-(7)) As a rule, the definitions of those exempted include unlisted businesses and payroll customers as defined in 31 CFR 1020.315 (b) (6) - (7). However, some businesses still do not qualify for the exemption; refer to 31 CFR 1020.315(e) (8) and the Monetary Trading Report Exemption section of this manual. 4. Determine whether the bank submits an electronic tax exemption report through the FinCEN Electronic Filing System to exempt customers, as determined by management, from the CTR. 5 report. Determine whether the bank maintains documentation to support non-listed businesses that the bank has specified as exempt from CTR reporting that does not receive more than 50 percent of total revenue from ineltrable business activities. 6. Assess whether ongoing and reasonable due diligence is carried out, including mandatory annual assessments, to determine if the customer is eligible to be identified as exempt from CTR reporting. Customers must meet the following requirements to be eligible for regulatory exemptions: There are regular 95FinCEN noted that when explaining the term regularly for the purposes of 31 CFR 1020.315(b) (6) (ii): [The Bank] may assign another eligible customer to waive phase II after the customer has within one year of performing the year or multiple transactions cash can be reported. Reference 73 Fed. Reg. 74010, 74014 (December 5, 2008). currency transactions in excess of $10,000 (including withdrawals to pay domestic employees in the currency in the case of a payroll client). Established or organized under the laws of the United States or a state, or registered and eligible to do business in the United States or a state. Maintain bank transactions for at least two months (or before the expiration of the two-month period if conducted a risk-based analysis of the client that allows it to form and record a reasonable belief that the client has a legitimate business purpose to conduct large currency transactions regularly). Check out Transaction 7. On the basis of risk assessment, pre-inspection reports and review of the bank's audit results, select a sample of the Bank's Exempt Person Designation (DOEP) report to check compliance with regulatory requirements (e.g., only eligible businesses are exempt from and maintain adequate supporting documentation). 8. On the basis of complete inspection procedures, including transaction inspection, a conclusion on the possibility of policies, procedures and procedures to meet the regulatory requirements related to exemption from currency transaction reporting. Page 2 Goals. Assess financial institutions' compliance with regulatory and regulatory requirements for the Special Information Sharing Process to prevent money laundering and terrorist activity (section 314 Information Requests). On September 26, 2002, the final provisions (31 CFR 103,100 and 31 CFR 103110) implemented section 314 of the U.S. PATRIOT Act that went into effect. Regulations have established information-sharing procedures to prevent money laundering and terrorism. On February 5, 2010, FinCEN amended regulations that allow state, local law enforcement, and some foreign law enforcement agencies to access the information-sharing program.96 Reference 75 Fed. Reg. 6560 (February 10, 2010). Sharing information between law enforcement and financial institutions - Section 314(a) of the U.S. PATRIOT Act (31 CFR 1010.520) A federal, state, local, or foreign law enforcement agency must come from a jurisdiction that is a party to the Mutual Legal Assistance Agreement between the United States and the European Union. Id. at 6560-61. Law enforcement agencies investigating terrorist activity or money laundering may require FinCEN to attract, on its behalf, some information from a financial institutions or a group of financial institutions. Law enforcement agencies must provide a written certificate to FinCEN c authentically c authentically that there is credible evidence of reasonable involvement or suspicion of involvement in terrorist activity or money laundering for each individual, organization or organization to whom law enforcement is seeking information. Law enforcement must also provide specific identities, such as date of birth and address, that allow a financial organization to distinguish between common or similar names. After receiving a complete written certificate from law enforcement, FinCEN may ask the financial institutions to search their records to determine whether the organization maintains or maintains an account or has engaged in transactions with any individual , which specific organization or organization. Search Request Upon receiving an information request,98If the request contains suspect, it is often referred to as a 314(a) list. a financial institutions must conduct a search of its records in order to identify the account or transaction of a named suspect. Unless otherwise instructed by an information request, financial institutions must search their records for existing accounts, accounts maintained for the previous 12 months, and transactions made outside the account by or on behalf of a named suspect in the previous six months. Financial institutions must search their records and report any positive matches to FinCEN within 14 days, unless otherwise specified in the information request. In March 2005, FinCEN began posting a list of 314(a) topics through the Web-based Secure Information Sharing System 314(a). Every two weeks, or more often if an emergency request is transmitted, the financial institutions' specified contact point(s) will receive notice from FinCEN that there are new posts to FinCEN's secure website. Point of contact will be able to access the current section 314(a) subject list (and a previous one) and download files in different formats to search. Financial institutions should report all positive matches through the Secure Information Sharing System (SISS). FinCEN has provided financial institutions with General Guidance and FAQs related to process 314(a). Unless otherwise instructed by an information request, financial institutions must seek the records specified in the General Guidelines.99 For example, in relation to money transfers, the General Guidelines state that, unless there are guidelines for a specific state requirement 314(a) other, banks are required to search for money transfer records maintained under 31 CFR 1010.410, to determine whether the named object is the originater/transfere for which the bank is the financial institutions of the originater/originater or beneficiary/recipient of the money transfer for which the bank is the beneficiary/financial organization of the recipient. General instructions or FAQs are provided to financial institutions on SISS.100 General Instructions and FAQs can also be obtained by calling fincen resource center toll-free (800) 767-2825 or (703) 905-3591 or by emailing FRC@fincen.gov. If a financial institutions determines any account or transaction, the financial institutions must report to FinCEN that the account or transaction has matched results. No details were provided to FinCEN other than the fact that the financial institutions had matched results. A negative reaction is not necessary. A financial institutions may provide a 314(a) subject list to a third-party service provider or provider to perform or facilitate records searches as long as the organization takes the necessary steps, through the use of agreements or procedures, to ensure that third parties protect and maintain the confidentiality of Believe. According to the FAQs available on SISS, if a the organization that received the 314(a) subject list through SISS did not perform or complete a search on one or more requests for information received in the previous 12 months, it must immediately get the previous request from FinCEN and perform a pre-search of its records.101The financial institutions should contact FinCEN's 314 Program Office by emailing sys314a@fincen.gov to get previous requests for information. If the financial institutions discover a positive combination while performing a reactively search, it will contact the Free Office Program Number 314 at (866) 326-8314. Financial institutions must respond with positive results within 14 days of receiving the prior request for information; however, if the results of a re-search do not match positively, no

further action is required. A financial institutions are not required to perform a re-search in relation to requests to share information transmitted more than 12 months prior to the date of discovery that the financial institutions did not perform or complete searches as previously requested. In addition, when performing a re-search, financial institutions are not required to search for records created after the original information request date. Restrictions on use and security Financial institutions should develop and implement comprehensive policies, procedures and procedures to meet section 314(a) requirements. This provision restricts the use of information provided in a section 314(a) request (31 CFR 1010.520(b)(3)(iv)). A financial institutions may only use the information to report the information necessary to FinCEN, to determine whether to set up or maintain an account or to participate in a transaction or to assist in BSA/AML compliance. Although the 314(a) subject list can be used to determine whether to set up or maintain an account, FinCEN discourages financial institutions from using this as the sole factor in making a decision to do so unless otherwise specifically stated. Unlike ofac lists, section 314(a) of the subject list is not permanently viewed. In fact, section 314(a) the subject list usually involves a one-time request and is not updated or corrected if an investigation is dropped, the prosecution is denied, or a topic is vindicated. Moreover, the name does not correspond to the person convicted or prosecuted; instead, an object 314 (a) should only be reasonable doubt based on credible evidence of involvement in acts of terrorism or money laundering. Furthermore, FinCEN recommends that the included in the section 314(a) subject list is not the only factor used to determine whether to file SAR. Financial institutions should establish a process to determine when and if SAR should be filed. Refer to the core overview, Suspicious Activity Report, page 60, for further instructions. Actions taken in accordance with the information provided in the request from FinCEN do not affect obliged to comply with all OFAC rules and regulations and not to affect the financial institutions' obligations to meet any legal process. In addition, actions taken to meet the requirements do not diminish the financial institutions' SAR filing obligations and immediately notify law enforcement, if necessary, in accordance with applicable laws and regulations. A financial institutions cannot disclose to any person, other than FinCEN, the main banking regulator of the organization or law enforcement agency that requests information on behalf of FinCEN, the fact that FinCEN has requested or collected information. A financial institutions should specify one or more contact points to receive requests for information. FinCEN has stated that a group of affiliate financial institutions can set up a point of contact to distribute the 314 topic list (a) in response to requests. However, topic list 314(a) cannot be shared with any foreign office, branch or branch (unless otherwise specifically stated) and the list cannot be shared with branches or subsidiaries of the bank holding companies, if the affiliates or subsidiaries are not financial institutions as described in 31 USC 5312 (a) (2). Each financial institutions must maintain adequate procedures to protect the security and security of requests from FinCEN. Procedures to ensure confidentiality will be fully reviewed if financial institutions apply procedures similar to the procedures established to comply with section 501 of the Gramm-Leach-Bliley Act (15 USC 6801) to protect customers' nonp public personal information. Financial institutions may keep logs of all requests section 314(a) received and any positive matches identified and reported to FinCEN. Additionally, documents that all necessary searches have been performed are essential. Banks can print or store self-verified search documents from Web-based SISS 314(a) for each 314(a) subject list transmission. Additionally, a list of subject reactions can be printed for documentation purposes. The topic feedback list shows the total number of positive feedback sent to FinCEN for that transmission, the date of transmission, the date of sending and the number of followers, and the subject name with positive hits. If the financial institutions choose to maintain copies of section 314(a) requirements, it should not be criticized for doing so, as long as it appropriately protects them and protects their security. Audits must include an assessment of compliance with these principles within their scope. FinCEN regularly updates its list of recent search transmissions, including information about the date of transmission, tracking number, and audience numbers listed in the newsletter.102 This list, nicknamed Share Law Enforcement Information with the Financial Industry, is available on section 314(a) of the Site. This list contains information about each search request that was transmitted from January 4, 2005, and updated after each transmission. Banks and examiners can review this list to verify that search requests have been received. Each bank should contact its main federal regulator for guidance to ensure it gets section 314(a) of the subject list and to update the contact information.103Refer to the FinCEN website for section 314(a) contacts for each major regulatory body. Voluntary information sharing — Section 314(b) of the USA WATER ACT (31 CFR 1010540) Section 314(b) encourages financial institutions10431 CFR1010.540 generally defines financial institutions as any financial institutions described in 31 USC 5312 (a) (2) are required to establish and maintain an AML compliance program. Refer to FinCEN's Information Sheet section 314(b) of October 2013 for general information. and the association of financial institutions105In July 2012, FinCEN issued an administrative ruling clarifying the meaning of the association of financial institutions. See FIN-2012-R006. in the United States to share information to identify and report activities that may be related to terrorist activity or money laundering. Section 314(b) also provides specific protection from civil liability.106FinCEN has indicated that a financial organization participating in section 314(b) may share information relating to transactions that the organization suspects may be related to proceeds from one or more illegally specified activities (SUAs) and that the organization will remain in the protect the port of safety section 314 (b) from liability. Information relating to the SLA may be appropriately shared within a safe 314(b) within the financial institutions suspecting that the transaction may be related to the proceeds of one or more SLA's and that the purpose of sharing the information permitted under rule 314(b) is to identify and report activities that the financial institutions suspect may be related to possible terrorist activity or money laundering. Refer to the Permitted Scope of Information Sharing Guide mentioned in Section 314(b) Safe Harbor of the US PATRIOT Act, FIN-2009-G002, June 16, 2009. To take advantage of this legally safe port from liability, a financial institutions or association must notify FinCEN of its intention to participate in information sharing and that it has established and will maintain adequate procedures to protect the confidentiality and confidentiality of the information. Non-compliance with the requirements of 31 CFR 1010.540 will result in a loss of secure port protection for information sharing and may result in a violation of privacy laws or other laws and regulations. If a financial institutions chooses to voluntarily participate in section 314(b), policies, procedures and processes need to be developed and implemented to share and receive information. Information sharing notices are effective for a when submitting a notice form (initial or renewal) available on the FinCEN website. Financial institutions should specify a point of contact to receive and provide information. A financial institutions should establish a process for sending and receiving requests to share information. In addition, a financial institutions must take reasonable steps to verify that other financial institutions or associations of financial institutions with which financial institutions intend to share information have also sent the necessary notice to FinCEN. FinCEN provides financial institutions with access to their list of other participating financial institutions and related contact information. If a financial institutions receives such information from another financial institutions, it must also restrict its use of the information and maintain its confidentiality and confidentiality (31 CFR 1010.540 (b) (4)). This information can only be used to identify and, where appropriate, report on money laundering and terrorism activities; to determine whether to set up or maintain an account; engage in a transaction; or to support BSA compliance. Procedures for ensuring confidentiality will be considered adequate if the financial institutions apply the same procedures as the one that the organization has established to comply with section 501 of the Gramm-Leach-Bliley Act (15 USC 6801) to protect the client's nonp public personal information. Safe harbors do not extend to information sharing across international borders. Additionally, section 314(b) does not allow a financial institutions to share SAR, nor does it allow financial institutions to disclose the existence or nonexistent existence of SAR. If a financial institutions shares information under section 314(b) about the subject of prepared or submitted SAR, the information shared should be limited to basic transactions and customer information. A financial institutions may use the information obtained under section 314(b) to determine whether to file sar, but the intention to prepare or file SAR cannot be shared with another financial institutions. Financial institutions should establish a process to determine when and if SAR should be filed. Actions taken in accordance with information obtained through voluntary information sharing do not affect the financial institutions' obligations to respond to any legal process. In addition, actions taken in response to information obtained through the voluntary information sharing process do not diminish the financial institutions' SAR filing obligations and immediately notify law enforcement, if necessary, in accordance with all applicable laws and regulations. Page 3 Goals. Assess financial institutions' compliance with regulatory and regulatory requirements for the Special Information Sharing Process to prevent money laundering and terrorist activity (section 314 Information Requests). Sharing information between laws and financial institutions (Section 314(a)) 1. Verify that the financial institutions are currently receiving section 314(a) requests from FinCEN or from an ally financial institutions acting as the point of contact of the subject financial institutions. If the financial institutions do not receive requests for information or change contact information, the financial institutions should update their contact information with the main regulatory authorities in accordance with the instructions www.fincen.gov. 2. Verify that financial institutions have adequate policies, procedures and procedures for documenting compliance; maintain sufficient internal control; provide ongoing training; and independently check compliance with 31 CFR 1010.520, implementing section 314(a) of the U.S. PATRIOT Act. At a minimum, the procedure should be done as follows: Specify a point of contact to receive the request for information. Ensure that the confidentiality of the requested information is protected. Set up a process to meet FinCEN requirements. Establish a process to determine whether sar should be filed and when. 3. Determine whether the search policies, procedures and procedures used by financial institutions to meet section 314(a) requirements are comprehensive and include all records identified in the General Guidelines for such requirements. General instructions include account searches maintained by the named topic for the previous 12 months and transactions made within the last six months. Financial institutions have 14 days from the date of transmission of the request for reply to the subject information form section 314(a). 4. If the financial institutions use a third-party provider to perform or facilitate the search, determine whether an agreement or procedure is in place to ensure confidentiality. 5. Review internal controls of financial institutions and determine whether their documents to prove compliance with section 314 (a) requirements are complete. This document may include, for example, the following: A copy of section 314(a) required. The log records the tracking numbers and includes the log out column. A copy of the search self-verification document created by SISS. If appropriate, request documentation from FinCEN regarding the bank's SISS access history. For positive matches, copies of the form are returned to FinCEN (e.g., A topic response list created by SISS) and supporting documentation must be retained. Voluntary information sharing (Section 314(b)) 6. Determine if the financial institutions have decided to voluntarily share information. If so, verify that the financial institutions submitted a notice form with FinCEN and provide an effective date for sharing the information within the previous 12 months. 7. Verify that financial institutions have policies, procedures and procedures for sharing information and receiving shared information, as stipulated in 31 CFR 1010.540, section 314(b) of the U.S. PATRIOT Act. 8. Financial institutions that voluntarily share information should have policies, procedures and procedures in recognition of compliance; maintain full internal control; provide ongoing training; and independently check compliance with 31 CFR 1010.540. At a minimum, the procedure should: Specify a point of contact to receive and provide information. Ensure the protection and security of the information received and the information requested. Establish a process for sending and responding to requests, including ensuring that other parties to whom the financial institutions intend to share information (including affiliates) have submitted appropriate notices. Establish procedures to determine whether or not sar should be filed and when. 9. If the financial institutions are sharing information with other organizations and do not follow the procedures outlined in 31 CFR 1010.540(b), notify the examiner to review the privacy rules. 10. By reviewing financial institutions' documents (including account analysis) on a sample of information shared and received, assessing how financial institutions determine whether SAR is covered by warranty. Financial institutions are not required to submit SARs only on the basis of information obtained through the voluntary information sharing process section 314(b). In fact, information obtained through the voluntary information sharing process section 314(b) may allow financial institutions to determine that there is no SAR required for initial transactions that may seem suspicious. Financial institutions should review account activity in determining whether SAR is covered by warranty. Check out Transaction 11. On the basis of risk assessment, pre-inspection report, and review of financial institutions' audit results, select a sample of appropriate results or recent requirements to determine if the following requirements have been met: Financial institutions' policies, procedures, and procedures allow financial institutions to search all identified records general guidelines for section 314 (a) requirements. Such processes can be electronic, manually, or both. Financial institutions look for appropriate records for each information request received. For positive matches: Verify that feedback was provided to FinCEN within the specified time period (31 CFR 1010.520(b)(3)(ii)). Review financial institutions' documentation (including account analysis) to assess how financial institutions determine whether SAR is covered by warranty. Financial institutions are not required to file SARs only on a combined basis with a named topic; instead, account activity should be reviewed in determining whether SAR is covered by warranty. Financial institutions use the information only in the way and for the permitted purposes and keep it safe and secure (31 CFR 1010.520 (b) (3) (iv)). (This request may be through discussions with management.) 12. On the basis of complete inspection procedures, including transaction inspection, a conclusion on the possibility of policies, procedures and procedures to meet the regulatory requirements related to information sharing. Page 4 Goals. Assess the bank's compliance with regulatory and regulatory requirements for recording information necessary for the purchase and sale of monetary instruments in currencies in amounts between $3,000 and $10,000, including. This section includes regulatory requirements set by the BSA. Refer to the extension of this manual for more discussions and procedures on the risk of money laundering specifically for buying and selling the activities of currency instruments. Banks sell a variety of currency instruments (e.g. bank cheques or drafts, including foreign drafts, money orders, cashier's checks, and traveler's checks) in exchange for currency. Buying these tools for less than $10,000 is a common method used by money launderers to evade large currency trading reporting requirements. After converting from currency, criminals often deposit these tools into account with other banks to facilitate the transfer of funds through the payment system. In many cases, the people involved do not have an account with the bank from which the tools are purchased. Buyer Verification Under 31 CFR 1010415 banks are required to verify the identities of buyers of currency instruments for currencies in amounts between $3,000 and $10,000, including, and to maintain records of all such sales. Banks can verify that the currency instrument buyer is the deposit account owner with information that identifies the record with the bank or bank can verify the identity of the buyer by viewing an identification form containing the name and address of the customer and the financial community accepted as a means of identification when withdrawing cheques to non-customers are customers. The bank must have more information for buyers who do not have a deposit account. The method used to verify the identity of the buyer must be recorded. Acceptable Identification U.S. Treasury Department Administrative Judgment 92-1 provides guidance on how a bank can verify the identity of an elderly or disabled customer without acceptable forms of normal identification. The bank may accept Social Security, Medicare, or Medicaid cards along with another form of documentation bearing the customer's name and address. Additional forms of documentation include utility bills, tax bills, or voter registration cards. The alternative form of identification a bank decides to accept should be included in its official policies, procedures and processes. Contemporary purchases Purchases at the same time with similar or different types of tools with a total value of $3,000 or more must be considered a purchase. Multiple purchases in one business day $3,000 or more must be summed up and considered a purchase if the bank has knowledge that the purchase has occurred. Buy currency instruments indirectly Banks can implement a policy that requires customers who are deposit account owners and want to purchase currency instruments for between $3,000 and $10,000 in currency to deposit the first currency into their deposit account. Nothing in the BSA or its implementation regulations prohibits a bank from instituting such a policy. However, FinCEN implements the Position108FinCEN Guidelines for the Explanation of Financial Institutions' Policies regarding record-holding requirements pursuing 31 CFR 103.29, November 2002. that when a client purchases a currency instrument in the amount of $3,000 to $10,000 in the currency that the client first deposits into the client's account, the transaction is still subject to the record-storing requirements of 31 CFR 1010.415. This requirement applies whether the transaction is made in accordance with the bank's established policy or at the request of the customer. Generally, when a bank sells currency instruments to deposit account owners, the bank will maintain most of the information required by 31 CFR 1010415 during its normal business. Requirements for storing and keeping records According to 31 CFR 1010.415, the bank's sales records must contain at least the following information: If the buyer has a deposit account with the bank: Buyer's name. Date of purchase. Types of buying tools. The serial number of each tool purchased. The dollar amount of each instrument is purchased in currency. Specific identifying information, if any.109The bank must verify that the person is the deposit account owner or must verify the identity of that person. Verification can be through a signature card or file or other record at the bank, as long as the name and address of the deposit account owner has been previously verified and that information has been recorded on a signature card or other file or profile, or by checking documents that are generally accepted in the banking community and contain the person's name and address Buy. If the identity of the deposit account owner has not been verified before, the bank will record specific identifying information (e.g. issuance status and driver's license number) of the document examined. If the buyer does not have a deposit account with the bank: The buyer's name and address. Social Security or the buyer's alien identification number. Buyer's date of birth. Date of purchase. Types of buying tools. The serial number of each tool purchased. The dollar amount of each buying instrument. Specific identification information to verify the identity of the buyer (e.g. issue status and number on driver's license). If the buyer is unable to provide the necessary information at the time transaction or through the bank's previously verified record, the transaction will be rejected. Records of the sale of currency instruments must be kept for five years and available to the appropriate authorities as required. Page 5 Goals. Assess the bank's compliance with regulatory and regulatory requirements for recording information necessary for the purchase and sale of monetary instruments in currencies in amounts between $3,000 and $10,000, including. This section includes regulatory requirements set by the BSA. Refer to the extension of this manual for more discussions and procedures on the risk of money laundering specifically for buying and selling the activities of currency instruments. 1. Determine whether the bank maintains the necessary records (in a manual or an automated system) to sell bank cheques or drafts including foreign drafts, checks of cashiers, money orders, and checks of tourists for currency in amounts between $3,000 and $10,000 , including, for buyers with deposit accounts with banks. 2. Determine whether the bank's policies, procedures and procedures allow the sale of currency instruments to buyers who do not have a deposit account with the bank (other than the customer): If so, determine whether the bank maintains a record of requesting the sale of currency instruments to unauthorized users. If not allowed, determine whether the bank allows sales on an exception basis. Check transaction 3. On the basis of risk assessment, pre-inspection report and review of the bank's audit results, select a currency instrument template sold in currencies in the amount of $3,000 to $10,000, including, to determine whether the bank has been, verify and retain the necessary records to ensure compliance with regulatory requirements. 4. On the basis of complete inspection procedures, including transaction inspection, a conclusion on the possibility of policies, procedures and procedures to meet the regulatory requirements related to the purchase and sale of monetary instruments. 5. On the basis of previous conclusions and risks related to the operation of the bank in this field, conduct extensive inspection procedures, if necessary. Page 6 Goals. Assess the bank's compliance with regulatory and regulatory requirements for money transfers. This section includes regulatory requirements as set out in the BSA. Refer to the extensions of this manual for discussions and procedures related to money laundering risks specific to money transfer activities. The money transfer system allows instant money transfers, including domestic and cross-border money transfers. Therefore, these systems may present an attractive method for disguising funds derived from illegal activity. BSA was amended by the Annunzio-Wylie Anti-Money Laundering Act of 1992 to authorize the U.S. Department of the Department of the money transfers. In 1995, the U.S. Treasury Department and the Federal Reserve System Governors' Council issued a final rule on record-storing requirements related to bank orders (31 CFR 1010,410). 11031 CFR 1020.410(a) is a record-store rule for banks and 31 CFR 1010.410 (e) imposes similar requirements on non-bank financial institutions participating in money transfers. The procedures in this core overview only address the rules for banks in 31 CFR 1020.410(a). The rule that requires each bank to participate in 111Funds transfers is determined according to 31 CFR 1010,100. Money transfers are governed by the Electronic Money Transfer Act of 1978, as well as any other money transfers made through an automated clearing house, automated cash machine or point-of-sale system, are excluded from this definition and are exempt from the requirements of 31 CFR 1020410 (a) and 31 CFR 1010.410 (e) and (f). to collect and retain certain information relating to transfers of $3,000 or more. 11231 CFR 1020.410(a) (6) provides exceptions for money transfer requests. Transfers in which both the originater and the beneficiary are the same person and the originater's bank and the beneficiary's bank are the same bank that is not subject to records-storing requirements for money transfers. In addition, exceptions are provided from record-keeper requirements for transfers in which the originater and beneficiary are: a bank; a domestic subsidiary owned by a bank with charter capital in the United States; a broker or stockbroker; a domestic subsidiary owned by a broker or securities agent; United States; state or local governments; or a federal, state, or local government agency or tool. The information required to be collected and retained depends on the bank's role in the specific transfer of funds (the initiated bank, intermediary bank or the beneficiary's bank). 113Th of these terms are defined in 31 CFR 1010,100 . Requirements may also vary depending on whether the originater or beneficiary is the bank's established customer and whether the payment order is made directly or otherwise. Also in 1995, the U.S. Department of the Financial Service issued a final rule that requires all financial institutions to include certain information in transmission orders for money transfers of $3,000 or more (31 CFR 1010,410). 114The rules apply to both banks and non-banks (31 CFR 1010.410(f). Because it is broader in scope, the Travel Rules use more extensive terms, such as commands instead of payment orders and financial institutions of the transmiter instead of the originating bank. Broader terms include bank-specific terms. This requirement is often referred to as the Travel Rule. Responsibilities of storage requirements originater's bank records For each payment order in the amount of $3,000 or more that the bank accepts as the originater's bank, the bank must have been and keep the following records (31 CFR CFR The name and address of the originater. The amount of the payment order. The date of the payment order. Any payment instructions. The identity of the beneficiary. As many of the following items as received with the payment order: The name and address of the beneficiary. Beneficiary's account number. Any other specific identity of the beneficiary. Additional record keeping requirements for customers are not established If the originater is not an established customer of the bank, the originater's bank must collect and retain the information listed above. In addition, the originater's bank must collect and retain other information, depending on whether the payment order is made directly. Payment order is made directly If the payment order is made directly, the originater's bank must verify the identity of the payment orderer before accepting the order. If a payment order is accepted, the originater's financial institutions must have and keep the following records: The name and address of the orderer. The type of identification is considered. Identification number (e.g., driver's license). The person's taxpayer identification number (TIN) (e.g., Social Security number (SSN) or employer identification number (EIN)) or, if there is no alien identification number or passport number and country of issued, or the symbol on the record lacks that number. If the originator's bank knows that the payment orderer is not the originator, the originator's bank must have and record the originator's TIN (e.g. SSN or EIN) or, if there is no alien identification number or passport number and issue country or missing symbol. Payment orders Are not made directly If the payment order is not made directly, the originater's bank must have and keep the following records: The name and address of the person who placed the payment order. Person's TIN (e.g. SSN or EIN) or, if not, a foreigner's identification number or passport number and issue country, or a symbol in the dossier about the lack or recording of a payment method (e.g. a check or credit card transaction) for money transfer. If the originator's bank knows that the payment orderer is not the originator, the originator's bank must have and record the originator's TIN (e.g. SSN or EIN) or, if there is no alien identification number or passport number and issue country or missing symbol. The retrieved information retained must be retrieved by reference to the originator's name. When the originater is the bank's established customer and has an account used for money transfers, the retained information must also be retrieved using the account number (31 CFR 1010.410 (a) (4)). Applications must be maintained for five years. Travel rule requirements For transfers of $3,000 or more, the player's financial institutions must include in the order of transmission at the time a command is sent to a receiving financial institutions (31 CFR 1010.410 (f) (1)): The name of the transmiter, and, if payment is ordered from an account, the transmiter's account number. The address of the machine. Number of transmission order. The day of the command order. The identity of the recipient's financial institutions. As many of the following items as received with the transmission order: The name and address of the recipient. The recipient's account number. Any other specific identity of the recipient. The name and address or digital identity of the financial institutions of the player. There are no records storage requirements in the Travel Rules. Responsibilities of the Intermediary Record Keeping Request For each payment order of $3,000 or more that a bank accepts as an intermediary bank, the bank must retain a record of the payment order. Travel rule requirements For transfers of $3,000 or more, the intermediary financial institutions must include the following information if received from the sender in the order of transmission at the time the order is sent to a receiving financial institutions (31 CFR 1010.410 (f) (2)): The name and account number of the transmit transmit. The address of the machine. Number of transmission order. The day of the command order. The identity of the recipient's financial institutions. As many of the following items as received with the transmission order: The name and address of the recipient. The recipient's account number. Any other specific identity of the recipient. The name and address or digital identity of the financial institutions of the player. Intermediary financial institutions must transfer all information received from the financial institutions of the previous giveer or financial institutions, but they are not obliged to have the information not provided by the financial institutions of the previous broadcasting machine or financial institutions. Liability of the beneficiary's bank record keeping requirements For each payment order of $3,000 or more that the bank accepts as the beneficiary's bank, the bank must retain the record of the payment order. If the beneficiary is not an established customer of the bank, the beneficiary's organization must with retain the following information for each payment order of $3,000 or more. Proceeds are delivered directly If the proceeds are delivered directly to the beneficiary or his or her representative or agent, the organization must verify the identity of the recipient and keep the record as follows: Name and address. The type of document to be reviewed. Number of ID Documents. The person's TIN, or, if not, the alien identification number or passport number and issue country, or the symbol in the missing record. If the educational institution knows that the recipient of the proceeds is not the beneficiary, the educational institution must and keep records of the beneficiary's name and address, as well as the beneficiary's identities. Proceeds Not delivered directly If the proceeds are not delivered directly, the organization must retain a copy of the cheque or other instrument used to make the payment, or the organization must record the information on the tool. The organization must also record the name and address of the person to whom it was sent. The retrieved information retained must be retrieved by reference to the beneficiary's name. When the beneficiary is the established customer of the organization and has the account used for money transfer, the retained information must also be retrieved by account number (31 CFR 1020410 (a) (4)). There are no travel rule requirements for beneficiary banks. Abbreviations and addresses Although travel rules do not allow the use of encrypted names or pseudonyms, this rule allows the use of abbreviations, names that reflect the different accounts of a company (e.g. XYZ Salary Account) and commercial and the assumed name of a business (business as) or the names of unsused departments or departments of the business karma. Customer Address The term address, as used in 31 CFR 1010.410(f), is not defined. Previously issued instructions from FinCEN were understood not to allow the use of mailing addresses in transmission order when a street address is known to the transmiter's financial institutions. However, on November 28, 2003, the Notice of Federal Registration, 11568 Fed. Reg. 66708 (November 23, 2003). FinCEN has issued a regulatory explanation spokesman assuming that the Travel Rules should allow the use of mailing addresses, including post boxes, in the case of transmit orders transmitted in certain circumstances. The interpreter clearly states that, for the purposes of 31 CFR 1010.410(f), the term address means that the street address of the generator or the address of the generator is maintained in the financial institutions' automatic CIF (such as the address mail including a post box) as long as the organization maintains the address of the generator 116Consistent with 31 CFR 1020.220 , an address for the purposes of the Travel Rules as follows: for an individual, the address is a residential or business street address, army post box or Fleet Post Box or residential or business street address of a relative or other contact for those who do not have a residential or business address. For a person who is not an individual (such as a company, partnership, or trust), the address is a primary place of business, local office, or other physical location. However, while 31 CFR 102020220 applies only to new customers opening accounts on or after October 1, 2003, and while the money transfer waiver rule from the account definition, for banks, the Travel Rules apply only to all transfers of $3,000 or more , whether the machine is a customer for a purpose or not 31 CFR 1020220. information and address information can be retrieved at the request of law enforcement. Page 7 Goals. Assess the bank's compliance with regulatory and regulatory requirements for money transfers. This section includes regulatory requirements as set out in the BSA. Refer to the extensions of this manual for discussions and procedures related to money laundering risks specific to money transfer activities. 1. Verify that the bank has received and maintained appropriate records to comply with 31 CFR 1020.410(a). 2. Verify that the bank transmits payment information as required by 31 CFR 1010.410(f) (Travel Rules). 3. Verify that the bank filed the CTR upon receiving the currency or dispersed in a transfer in excess of $10,000 (31 CFR 1010311). 4. If the bank sends or receives money transfers to or from organizations in other countries, especially those with strict privacy and security laws, evaluate whether the bank has policies, procedures and procedures to determine if the amount, frequency of transfer and country of origin or destination is consistent with the nature of the business or occupation customer's business or not. Check trades 5. On the basis of risk assessment, pre-inspection report and review of the bank's audit results, select a transfer form to be processed as the originater's bank, intermediary bank and beneficiary's bank to ensure the organization collects, maintains or transmits the necessary information , depending on the organization's role in the transfer. 6. On the basis of completed inspection procedures, including transaction inspection, a conclusion on the possibility of policies, procedures and procedures to meet the regulatory requirements related to money transfer. 7. On the basis of previous conclusions and risks related to the bank's activities in this field, conduct extensive inspection procedures, if necessary. Page 8 Goals. Assess the bank's compliance with regulatory and regulatory requirements for agent accounts for foreign banks, storage of foreign agent account records and due diligence programs for detecting and reporting money laundering and suspicious activity. Assess the bank's compliance with the Iran Sanctions, Accountability and Comprehensive Divestment Act (CISADA), if applicable. Refer to the extension of the manual for discussing and examining procedures related to the specific risk of money laundering related to foreign agent accounts. One of the central goals of the U.S. PATRIOT Act is to protect access to the U.S. financial system by requesting certain records, reports, and due diligence programs for foreign correspondent accounts. In addition, the US PATRIOT Act prohibits accounts with foreign shell banks. Foreign correspondent accounts, as noted in previous U.S. Senate investigative reports, 117Correspondent Banking: A Gateway for Money Laundering. Refer to the Hearing Institute 107-84. Report page 273 of episode 1 of the hearing file titled The Role of U.S. Bank agents in international money laundering, held on March 1, 2, and 6, 2001. is a gateway to the U.S. financial system. This section of the manual includes regulatory requirements established by sections 312, 313, and 319(b) of the U.S. PATRIOT Act and by provisions implemented in 31 CFR 1010.100, 1010.610, 1010.630, and 1010.670. Additional discussions and procedures regarding money laundering risks specific to foreign agency banking activities, such as large currency quantity shipments, bag operations, draft U.S. dollars and account payments, are included in the extensions. Prohibition of offshore banking and storage of offshore agent accounts For the purposes of 31 CFR 1010.630 and 1010670, an agent account is an account established by an offshore bank to receive deposits from, or to make payment or other disbursement on behalf of foreign banks , or to process other financial transactions involving foreign banks. An account means any formal banking or business relationship established to provide services, transactions and other financial transactions on a regular basis. It includes on-demand deposits, savings deposits or trading accounts or other assets and credit accounts or other credit extensions (31 CFR 1010605 (c)). Accounts maintained by offshore banks for financial institutions covered by the rules are not agent accounts subject to this provision. 11871 Fed. Reg. 499. FinCEN has issued translated guidelines, Applying the Agent Account Rules to present the transfer instruments received by an insured financial institutions for payment, FIN-2008-G001, January 30, 2008, which states, In the course of normal business, an insured financial institutions may receive negotiating tools for payment from an organization foreign finance for which it maintains correspondent relationships. FinCEN does not consider the presentation of transactions according to the transaction of a transfer instrument to a foreign payment organization - either directly or through a clearing facility - as the establishment of a formal banking or business relationship by an insured financial institutions for purposes of complying with agency account rules. Under 31 CFR 1010630, a bank is prohibited from establishing, maintaining, managing or managing agent accounts in the United States for or on behalf of a foreign shell bank. A foreign shell bank is defined as an offshore bank without a physical presence in any country. 119 Physical presence means a place of business: - Maintained by an offshore bank. - Located at a fixed address (not just an electronic address or a post box) in a country where foreign financial institutions are permitted to conduct banking activities, at which the venue Foreign finance: - Use one or more people on a full-time basis. time. Maintain operational records related to your banking activities. - Subject to inspection by the banking agency which has licensed foreign financial institutions to carry out banking activities. One exception, however, is allowing a bank to maintain an agent account for an offshore shell bank that is a regulated branch. 120A affiliate regulation is a shell bank that is allyed with a deposit deposition organization, credit union, or foreign bank that maintains a physical presence in the United States or in other jurisdictions. Regulated banking is also subject to the supervision of the banking agency regulating the affiliate. 31 CFR 1010.6 30 also requires a bank to take reasonable steps to ensure that any agent account set up, maintained, managed or managed in the United States for an offshore bank is not used by that foreign bank to provide indirect banking services to foreign banks. Certification A bank that maintains an agent account in the United States for an offshore bank must maintain records in the United States that identify the owner of each offshore bank. 121To minimize the burden of record-storing, ownership information is not necessary for foreign financial institutions to submit a form of FR Y-7 (Annual Report of Foreign Banking Institutions) to the Federal Reserve or to those foreign financial institutions that are publicly traded. Public transactions are stocks traded on exchanges or organized over-the-top markets regulated by foreign securities agencies in accordance with section 3(a) (50) of the Securities Trading Law of 1934. A bank must also record the name and street address of a person residing in the United States and who is authorized to, and has agreed to, be an agent to accept the services of the legal process. 122 The service of the legal process means that agents are willing to accept legal documents, such as subpoenas, on behalf of offshore banks. Under 31 CFR 1010670, a bank must present these records within seven days of receiving a written request from a federal law enforcement officer. The U.S. Treasury Department, working with federal industry and banking and law enforcement agencies, has developed a certification process to assist banks in complying with record-storage terms. This process includes forms of certification and re-certification. While banks are not required to use these forms, a bank will be deemed in accordance with the regulations if it gets a complete form of certification from offshore banks and receives a reconst confirmation on or before the three-year anniversary of the initial or previous certification. 123Refer to Frequently Asked Questions, Foreign Bank Recertifications under 31 CFR 103177, FIN-2006-G003, 3 February 2006. Account closure This Regulation also includes specific regulations on when banks must get the information they need or close the agent account. Banks must (or re-certification) or get the necessary information within 30 calendar days from the date the account is set up and at least every three years there follow. If the bank is unable to get the necessary information, the bank must close all agent accounts with the offshore bank for a reasonable period of time commercially. Verification A bank should review the certifications to be reasonable and accurate. If a bank at any time knows, doubts or has reason to suspect that any information in the certificate (or re-certification) or any other information the bank relies on is no longer accurate, the bank must require the foreign bank to verify or correct it or the bank must take other appropriate measures to verify its precise determination. Therefore, banks should consider certifications for potential issues that may warrant further review, such as using post boxes or forwarding addresses. If the bank does not have the necessary information or repairs within 90 days, the bank must close the account within a reasonable commercial time. During this time, the bank must not allow the offshore bank to set up any new financial position or make any transactions through the account, in addition to the transactions necessary to close the account. In addition, the bank may not set up any other agent accounts for offshore banks until necessary information is available. The Bank must also retain the originals of any documents provided by the offshore bank and retain the originals or copies of any other documents relied upon for the purposes of regulation, for at least five years from the date the bank no longer maintains any agent accounts for offshore banking. Subpoena Pursuencies Pursuencies Section 319(b) of the U.S. WATER ACT, the Secretary of the Treasury or the Secretary of Justice may issue subpoenas or subpoenas to any foreign bank that maintains an agency account in the United States to get records related to that account , including records maintained abroad or to get records related to depositing money into offshore banks. If a foreign bank does not comply with a subpoena or does not initiate a lawsuit to dispute that subpoena, the Secretary of the Treasury or the Secretary of Justice (after consultation with each other) may, in writing notify, direct a bank to terminate its relationship with a foreign agency bank. If a bank does not terminate the agency relationship within ten days of receiving the notice, the bank may be fined a civil fine of up to $10,000 per day until the agent relationship ends. Federal Regulatory Agency AML filing requirements In addition, at the request of the federal regulator, the bank must provide or make available records regarding the compliance with the AML of the bank or one of its customers, within 120 hours of the time (31 USC 5318 (k) (2)). Special due diligence program for foreign correspondent accounts 312 of the U.S. PATRIOT Act added subs section (i) to BSA's 31 USC 5318. This subss section requires each U.S. financial institutions to set up, maintain, manage, or manage agent accounts in the United States for foreign financial institutions to implement certain AML measures for those accounts. Additionally, section 312 of the US PATRIOT Act provides for additional standards for agent accounts to be maintained for certain offshore banks. General Due diligence 31 CFR 1010.610(a) requires banks to establish an due diligence program that includes appropriate, specific, risk-based policies and, where necessary, enhanced policies, procedures, and controls designed to enable the bank to detect and report, on an ongoing basis, any known or suspected money laundering activity conducted through or in connection with any agency account established, maintained, managed or managed by a bank in the United States to a foreign financial institutions 124 Terms of foreign financial institutions as defined in 31 CFR 1010.605 (f) generally include : - An offshore bank. - Foreign branches or offices of banks, brokers/securities dealers, futures commission traders, introductory brokers or mutual funds. - Any other person held under foreign law, if located in the United States, will be a broker/agent in securities, futures commission merchants, introducing brokers, or mutual funds. - Any person held under foreign law engaged in the business and can be easily identified as, a currency agent or exchange or a money machine. (foreign agent account). Due diligence policies, procedures and controls must include the following policies, procedures, and controls: Determine if each of those offshore agent accounts is subject to EDD (refer to Advanced Due diligence below). The risk assessment of money laundering is presented by each of those offshore agent accounts. Apply risk-based procedures and controls to each foreign agent account that are appropriately designed to detect and report known or suspected money laundering activity, including periodically evaluating agent account activity sufficiently to determine consistency with information obtained about the account's expected type, purpose and activity. Risk assessment of foreign financial institutions. The bank's general due diligence program must include policies, procedures and procedures for assessing risks rated by customers of foreign financial institutions of the bank. The bank's resources are most appropriately directed to accounts that pose a significantly greater risk of money laundering. The bank's due diligence program should stipulate that the risk assessment of foreign agency accounts considers all relevant factors, including, if appropriate: The business nature of the foreign financial institutions and the markets in which it serves. The expected type, purpose and activity of the agent account Beyond. The nature and timing of relations with foreign financial institutions (and, if relevant, with any branch of a foreign financial institutions). AML and its supervisory regime have issued charters or licenses to foreign financial institutions and, to the extent that information relating to that jurisdiction are reasonablely available, on the jurisdiction to which any company is the owner of established foreign financial institutions or charters. Information is known or available to the bank in terms of aml records of foreign financial institutions, including public information in industry guidelines, periodo-time journals and major publications. Banks are not required to evaluate all of the above factors for each agent account. Monitoring foreign correspondent accounts. As part of the ongoing due diligence, banks should periodically review their offshore agent accounts. Monitoring will not, under normal circumstances, involve monitoring every transaction that takes place in the account, but should instead involve reviewing the account sufficiently to ensure that the bank can determine whether the nature and volume of account activity is consistent with information relating to the intended purpose of the account and the expected account activity and to ensure that the bank can fully identify suspicious transactions. An effective due diligence program will provide a wide range of due diligence measures, based on the bank's risk assessment for each offshore agent account. Therefore, the starting point for an effective due diligence program should be to decentralize the money laundering risk of each offshore agent account based on the bank's consideration of the relevant risk factors (such as the factors identified above) to determine which accounts may require increased measures. The due diligence program should identify risk factors that will ensure the organization conducts additional oversight or enhances monitoring of a particular account. Since due diligence is an ongoing process, a bank should take measures to ensure current account records and monitoring must be risk-based. Banks should consider whether risk profiles should be adjusted or suspicious activity reported when activity does not match records. Strengthening due diligence 31 CFR 1010.610(b) requires banks to establish policies, risk-based EDD procedures and controls when setting up, maintaining, managing or managing U.S.

agent accounts for certain foreign banks (as defined in 31 CFR 1010.610(c) operating under any or more of the following : Offshore banking license. 125The USA PATRIOT Act (31 USC 5318(i)(4)(A) and 31 CFR 1010.605(i) define an offshore banking license as a license to conduct banking activities that, as a condition of license, prohibit licensed institutions from conducting banking activities with citizens , or in the local currency of, the authority issued A foreign-issued banking license has been specified as not to cooperate with international AML guidelines or procedures by an inter-governmental group or organization to which the United States is a member, and which nomages U.S. representatives for the consensus group or organization. The Financial Action Task Force (FATF) is the only inter-governmental organization of which the United States as a member has appointed countries that do not cooperate with international anti-money laundering principles. The United States has agreed to all FATF nomeds so far. Bank licenses issued by foreign countries have been specified by the Minister of Finance as ensuring special measures due to money laundering concerns. If such an account is set up or maintained, 31 CFR 1010.610(b) requires the bank to establish EDD policies, procedures and controls to ensure that the bank, at a minimum, takes reasonable steps to: Identify, for any foreign bank with shares that are not publicly traded , the identity of each owner of the offshore bank and the nature and level of ownership interest of each of those owners. 127C ownership is any person who directly or indirectly owns, controls or has the right to vote of 10 percent or more of any securities of an offshore bank (31 CFR 1010610 (b) (3). Public trading means shares traded on exchanges or organized over-the-top markets administered by foreign securities authorities, as provided in section 3(a)(50) of the Securities Exchange Act of 1934 (15 USC 78c (a) (50)) (1010.610(b) (3). Guidelines on the collection and retention of beneficial ownership information, issued by FinCEN, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of Currency Control, the Office of Savings Supervision and the Securities and Exchange Commission , in consultation with the Futures Goods Trading Commission, in May 2010, the Guide reinforces existing regulatory expectations to get ownership information in favor of certain accounts and customer relationships. Enhanced account monitoring to protect against money laundering and identify and report any suspicious transactions under applicable laws and regulations. This increased oversight is to reflect the risk assessment of the account and will include, if appropriate: Collection and review of information relating to the foreign bank's anti-money laundering program to assess the risk of money laundering presented by the offshore bank's agency account. Monitor transactions to, from or through an agent account in a way that is properly designed to detect money laundering and suspicious activity. Get information from an offshore bank about the identity of any person authorized to direct transactions through any agent account through accounts, and sources and beneficial owners of funds or other assets in payment through the account. Determine whether the offshore bank to which the agent account is maintained in turn maintains an agency account for other foreign banks that use the agent account of the offshore bank and, if so, take reasonable steps to get relevant information to assess and minimize the risk of money laundering associated with the bank's agency account to other foreign banks, including, if appropriate, the identities of such offshore banks. In addition to the types of offshore banks defined in the regulation as EDD requirements, banks may find it appropriate to conduct additional due diligence measures on foreign financial institutions identified through the application of the bank's general due diligence program that poses a higher risk of money laundering. Such measures may include any or all elements of EDD specified in the regulation, in accordance with the risks ngested by specific offshore agent accounts. As noted in the above section on general due diligence, the bank's resources are most appropriately directed to accounts that pose a significantly greater risk of money laundering. Accordingly, in the event that the bank is otherwise required or determined that it is necessary to conduct EDD in relation to the offshore agent account, the bank may consider the risk assessment factors discussed in the general assessment when determining the level of EDD required and appropriate to minimize the risks presented. In particular, the anti-money laundering and supervision regime of the authority that issued the charter or license to the foreign financial institutions may be particularly suitable in determining the bank's nature and degree of risk handled by the foreign agent account and the extent to which EDD is applied. Special procedures when due diligence cannot implement the bank's due diligence policies, procedures and controls established under 31 CFR 1010.610 must include procedures to be followed in the event of an appropriate due diligence or EDD cannot be performed on a foreign agent account , including when the bank should: Refuse to open an account. Suspension of trading activity. File sar. Close the account. Iran's Comprehensive Act on Sanctions, Accountability and Divestment in 2010 the Iran Comprehensive Sanctions, Accountability and Divestment Act (CISADA) was signed into law on July 1, 2010. 128Pub. L. No. 111-195, 124 Statistics 1312 (2010). CISADA allows the Secretary of the Finance to prohibit or impose strict conditions on the opening or retention of U.S. agent accounts and payments through accounts to foreign financial institutions that the Minister determines have been intentionally engaged in activities that may be sanctioned. On October 11, 2011, FinCEN issued a final rule required to report under section 104(e)(1)(B) of CISADA (31 CFR 1060,300). 129Refer to 76 Fed. Reg. 62607 (October 11, 2011). Also available at the FinCEN website. It is important to note that FinCEN will call CISADA reporting requirements in very limited circumstances, when necessary, to elicit valuable information. The final rule requires U.S. banks to report information after receiving a written request from FinCEN: Whether a foreign bank maintains an agency account for an Iranian-linked financial institutions specified under the International Emergency Economic Powers Act (IEEPA); Whether the offshore bank has processed one or more transfers within the previous 90 calendar days for either on behalf of, directly or indirectly, an Iranian- linked financial institutions is specified under the IEEPA, in addition through an agency account; and whether the foreign bank processed one or more transfers within the previous 90 calendar days for either on behalf of, directly or indirectly, the Iranian Islamic Revolutionary Guard Corps (IRGC) or any agent or branch specified under the IEEPA. U.S. banks must report to FinCEN within 45 calendar days regardless of the foreign bank's response (e.g., positive feedback, negative reactions, incomplete feedback, or no response). If an information is received from a foreign bank after the scheduled 45-day period, the U.S. bank must report it to FinCEN within 10 calendar days after receiving it. The rule also requires U.S. banks to report for FinCEN cases in which the bank does not maintain an agent account for a specified offshore bank. In addition, the rule requires U.S. banks to require foreign banks to agree to notify them if the offshore bank then sets up a new agency account for an Iranian-linked financial institutions specified under the IEEPA at any time within 365 calendar days of the date the offshore bank initially responds. Reports relating to a new agency account for an Iranian-linked financial institutions specified under the IEEPA will be due within 10 days of receiving. FinCEN has developed a model certification form for a U.S. bank to provide offshore banking when complying with its requirements as required by the rule. 130 View the document on the FinCEN website. The use of the model certification form is optional. However, any alternative form used by a U.S. bank should require the same information as the model certification form. This Rule does not require the bank to take any action other than actions related to the collection of information regardless of the feedback received from the offshore bank and the request for information from FinCEN does not diminish the bank of any other regulatory requirements. The Bank should evaluate all information it knows about its customers under the risk-based BSA/AML compliance program to determine whether additional action or submit sar. The Bank will a copy of any report submitted to FinCEN and any supporting documents, including foreign bank certification or other responses to an investigation over a five-year period. Page 9 Goals. Assess the bank's compliance with regulatory and regulatory requirements for agent accounts for foreign banks, storage of foreign agent account records and due diligence programs for detecting and reporting money laundering and suspicious activity. Assess the bank's compliance with the Iran Sanctions, Accountability and Comprehensive Divestment Act (CISADA), if applicable. Refer to the extension of the manual for discussing and examining procedures related to the specific risk of money laundering related to foreign agent accounts. 1. Determine whether the bank is involved in a foreign agent bank. Prohibits offshore shell banks and offshore agent account storage 2. If so, review your bank's policies, procedures, and processes. At a minimum, policies, procedures and procedures must be implemented as follows: Prohibit transactions with foreign banks and appoint the party responsible for collecting, updating and managing certificates or information for foreign agent accounts. Identify foreign agent accounts and resolve the sending, monitoring, receiving and review of requests or requests for certification of information. Evaluation of the quality of information received in response to a request for certification or request for information. Determine whether to file sar and when. Maintain full internal control. Provides for continuous training. Independently check the bank's compliance with 31 CFR 1010,630. 3. Determine whether the bank is on the current certification dossier or current information (otherwise it will include the information included in a certificate) for each foreign agent account to determine whether the foreign partner is not a foreign shell bank (31 CFR 1010.610(a)). 4. Where the bank has a foreign branch, determine whether the bank has taken reasonable steps to ensure that any agent account maintained for the foreign branch of the foreign bank is not used to indirectly provide banking services to foreign banks. Special due diligence program for foreign correspondent account 5. Determine whether the bank has established a general due diligence program that includes appropriate, specific, risk-based and, as necessary, enhanced policies, procedures and controls for agent accounts established, maintained, managed or managed in the United States for foreign financial institutions (offshore agent accounts). The general due diligence program must be applied to each foreign agent account. Verify that due diligence policies, procedures and controls include: Determining whether any foreign agent accounts are subject to EDD (31 CFR 1010.610 (a) (1)). Risk assessment of money laundering presented by foreign reporters (31 CFR 1010.610(a)(2)). Apply risk-based procedures and controls to each foreign agent account that are appropriately designed to detect and report known or suspicious money laundering activity, including periodically evaluating agent account activity sufficiently to determine consistency with information obtained about the type, purpose and expected activity of the account (31 CFR 1010.610 (a) (3)). 6. Review the policies, procedures and due diligence procedures of the BSA/AML risk assessment adjustment program of foreign agent accounts (31 CFR 1010.610(a)). Verify that the bank's due diligence program considers the following factors, when appropriate, as criteria in risk assessment: The nature of the business activities of foreign financial institutions and the markets in which it serves. The expected type, purpose and operation of the foreign agent account. The nature and timing of the bank's relationship with foreign financial institutions and any branch of the bank. AML and its supervisory regime have issued charters or licenses to foreign financial institutions, and, to the extent that information relating to that jurisdiction is reasonably available, on the jurisdiction to which any company is the owner of established foreign financial institutions or charters. The information is known or reasonable available to the bank about the AML records of foreign financial institutions. 7. Ensure the program is designed to: Detect and report, on the basis of continuity, known or suspected money laundering activities. Periodically evaluate agent account activity to determine consistency with information obtained about the expected type, purpose and activity of the account. 8. For foreign banks subject to EDD, evaluate the criteria used by U.S. banks to protect against money laundering and report suspicious activity related to any agency accounts held by such foreign banks. Verify that the EDD procedures are applied to each partner account established for foreign banks operating under: Offshore banking licenses. A foreign-issued banking license has been specified as not to cooperate with international AML guidelines or procedures by an inter-governmental group or organization to which the United States is a member, and which nomages U.S. representatives for the consensus group or organization. A banking license issued by a foreign country has been specified by the Minister of Finance as ensuring special measures due to AML's concerns. 9. Review the bank's policies, procedures and procedures and determine if they include reasonable steps to conduct enhanced monitoring of foreign agent accounts to protect against money laundering and identify and report any suspicious transactions under applicable laws and regulations (31 CFR 1010.610 (b) (1)). Verify that this enhanced oversight reflects risk assessment of each foreign agent account subject to such supervision and includes, if appropriate: Collection and review of information relating to the foreign bank's anti-money laundering program to assess the risk of money laundering presented by the offshore bank's agency account (31 CFR 1010.610 (b) (1) (i)). Monitor transactions to, from or through a partner account in a way that is properly designed to detect money laundering and suspicious activity (31 CFR 1010.610 (b) (1) (ii)). Get information from the offshore bank about the identity of any person authorized to direct transactions through any agent account payable through the account, and the sources and beneficial owners of funds or other assets in the payable (31 CFR 1010.610 (b) (1) (iii)). 10. Review the bank's policies, procedures and procedures to determine whether foreign agency banks are subject to EDD maintenance of agency accounts for other foreign banks, and, if so, determine whether the bank's policies, procedures and procedures include reasonable steps to get relevant information for assessment and reduction minimizing the risk of money laundering in relation to the agent account of the foreign agent bank to other foreign banks, including, if appropriate, the identity of foreign banks (31 CFR 1010.610 (b) (2)). 11. Determine whether policies, procedures and procedures require the bank to take reasonable steps to determine whether each owner has the right to vote of 10 percent or more of any securities of a foreign agent bank that is not publicly traded but which bank opens or maintains an account subject to EDD. For such accounts, evaluate the bank's policies, procedures and procedures to determine the interest rate of each of those owners (31 CFR 1010.610 (b) (3)). Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 report requires 12. If the bank has received a written request from FinCEN for a specified offshore bank, review the bank's policies, procedures and procedures to meet FinCEN's written requirements. It is important to note that FinCEN will call CISADA reporting requirements in very limited circumstances, when necessary, to elicit valuable information. At a minimum, policies, procedures and procedures must be implemented as follows: Meet fincen requirements within the specified time frame. Request the necessary information from foreign banks. Comply with record-keeper requirements. Allows changes to the client's risk rating or profile. Check offshore banking transactions Shell Prohibition and store 13 offshore agent accounts. On the basis of risk assessment, pre-inspection report and review of the bank's audit results, select an offshore bank account form. From the selected form, determine as follows: Whether the certification and information on the account are complete and reasonable. Whether the bank has enough evidence that it does not maintain accounts or indirectly provide services to foreign shell banks. For account closures, whether the closure is done within a reasonable period of time and the relationship is not re-established without good reason. Whether there are any federal law enforcement requests for information related to offshore agent accounts. If so, determine that the request was met in a timely manner. Whether the bank receives any official notice to close an offshore financial institutions account. 131 Official notice to close the account of a foreign financial institutions must be signed by the Secretary of the Finance or the Secretary of Justice of the United States (31 CFR 1010.670(d). If so, determine that the account has been closed within ten business days. Whether the bank retains, for five years from the date of account closure, the original of any documents provided by a foreign financial institutions, as well as the original or copies of any documents based on any reference to any summons or subpoena issued by a foreign financial institutions pursuing 31 CFR 1010.670. Special due diligence program for 14 foreign correspondent accounts. From a selected form, determine whether the bank complies with general due diligence policies, procedures and procedures for offshore agent accounts. It may be necessary to extend the form to include maintenance agent accounts for foreign financial institutions other than foreign banks (such as money players or currency exchanges), where appropriate. 15. From the original form, determine whether the bank has carried out EDD procedures for foreign banks operating under: Foreign banking licenses. A banking license issued by a foreign country has been specified as not to cooperate with international AML principles or procedures. A banking license issued by a foreign country has been specified by the Minister of Finance as ensuring special measures due to AML's concerns. 16. From the EDD account form, verify that the bank has taken reasonable steps, in accordance with the bank's policies, procedures and procedures, to: Determine, for any foreign bank with shares not publicly traded, the identity of each foreign bank owner has the right to vote of 10 percent or more of any type of securities the nature and extent of each owner's ownership interest. Increase monitoring of any accounts held by those banks to protect against money laundering and report suspicious activity. Determine whether the offshore bank provides an agency account to other foreign banks and, if so, get relevant information to assess and minimize the risk of money laundering associated with the agent account of the offshore bank to other foreign banks , including, if appropriate, the identities of such offshore banks. 17. On the basis of the inspection procedures all, including transactions form a conclusion on the completeity of policies, procedures, and processes to meet regulatory requirements related to offshore agency account records and due diligence. 18. On the basis of previous conclusions and risks related to the bank's activities in this field, conduct extensive inspection procedures, if necessary. Comprehensive Iran sanctions, accountability, and divestment act of the 2010 report requires if the bank has received a written request from FinCEN on a regulated offshore bank, the following transaction inspection procedures should be carried out: 19. If the bank does not use the CISADA certification form, determine whether the bank's reporting format captures the necessary information (31 CFR 1060.300(c)(1)). 20. Feedback verification is provided to FinCEN within the specified time frame (31 CFR 1060,300 (c) (2)). 21. Determine whether the bank maintains a copy of the submission report, any supporting documents, cisada certification form or response by the offshore bank to request information for a period of 5 years. Page 10 Goals. Assess whether the bank complies with regulatory and regulatory requirements to implement policies, procedures, and controls to detect and report money laundering and suspicious activity through private bank accounts established, managed, or maintained for non-Americans. You. Refer to the extension of the manual for discussing and examining procedures related to the specific money laundering risk associated with private banking. Private banking can be broadly defined as providing personal financial services to wealthy clients. Section 312 of the U.S. PATRIOT Act added subsc section (i) to BSA's 31 USC 5318. This subsus requires each U.S. financial institutions to establish, maintain, manage, or manage private U.S. bank accounts for a non-U.S. financial institutions. certain AML measures for these accounts. In particular, a bank must establish appropriate, specific and as necessary EDD policies, procedures and controls, designed to enable the bank to detect and report cases of money laundering through such accounts. In addition, section 312 missions enhanced oversight to detect and, where appropriate, report transactions that may involve proceeds from foreign corruption for private bank accounts that are required or maintained by or on behalf of a senior foreign political person or the direct family of the individual and close relatives. On January 4, 2006, FinCEN issued a final regulation (31 CFR 1010620) to comply with the private banking requirements of 31 USC 5318(i). The overview and audit procedures set out in this section are intended to evaluate the bank's due diligence program in relation to private bank accounts offered to non-Americans. You. Additional procedures for specific risk areas of the bank are included in the extensive inspection procedures, the Private Bank, the Private bank account For the purpose of 31 CFR 1010620, a private bank account is an account (or any combination of accounts) maintained at a bank that meets all three criteria: Request a minimum general deposit of funds or other assets not less than $1,000,000. Founded on behalf of or for the benefit of one or more non-Americans. those who are the direct or beneficial owners 132 Beneficial owners of the account means that an individual has a degree of control or enjoys funds or assets in the account, as a matter of fact, allowing the individual, directly or indirectly, to control, manage or direct the account. However, the ability to deposit funds into the account or the right to enjoy funds of the account without any corresponding authority to control, manage or direct the account (such as in the case of a minor beneficiary), does not make the individual a beneficial owner (31 CFR 1010.605(a). Guidelines on the collection and with retention of beneficial ownership information, issued by FinCEN, The Board of Governors of the Federal Reserve System (Federal Reserve), Federal Deposit Insurance Corporation (FDIC), National Credit Union Management (NCUA), Office of Currency Control (OCC), Office of Savings Supervision (OTS) and Securities and Exchange Commission (SEC), consulted with the U.S. Securities and Exchange Commission, in May 2010. This guide reinforces existing regulatory expectations to get ownership information that benefits certain accounts and customer relationships. of the account. Assigned to, or managed by, in whole or in part, an officer, employee, or agent of a bank that acts as a liaison between a financial institutions covered by regulations and the direct or beneficial owner of the account. For minimum deposit requirements, a private bank account is an account (or combined account) that requires a minimum deposit of no less than $1,000,000. A bank can offer a wide range of services known as private banking, and even if some (or any combination, or all) the bank's private banking services do not require a minimum deposit of no less than $1,000,000, these relationships are subject to a greater level of due diligence under the bank's risk-based BSA/AML compliance program but are not subject to 31 CFR 1010.620. Refer to the extended overview section, Private Bank, page 273, for further instructions. The One Bank Due diligence program must establish and maintain an due diligence program that includes policies, procedures, and controls that are appropriately designed to detect and report any known or suspicious money laundering or suspected activity made through or in connection with any private bank account for a non-U.S. account. person established, maintained, managed or managed in the United States by a The due diligence program must ensure that, at a minimum, take reasonable steps to do each of the following: Identify all anonymous and beneficial owners of private bank accounts. Determine whether the name or benefit owner of any private bank account is a senior foreign political person. Identify the source(s) of deposits to the private bank account and the purpose and intended use of the account. Review the operation of the account to ensure that it is consistent with the information obtained about the client's funds, and for the stated purpose and intended use of the account, and to file sar, if appropriate, to report any known or suspicious money laundering or suspected activity carried out , from or through a private bank account. Private bank account risk assessments for non-Americans Nature and the level of due diligence performed on private bank accounts for non-Americans who may vary for each client depending on the presence of potential risk factors. More extensive due diligence, for example, may be appropriate for new customers; clients operating in, or having money transmitted from or through, legal areas with weak AML controls; and clients have trading activities that are primarily currency-based (e.g., casinos or currency exchanges). Due diligence should also be commensurate with the size of the account. Accounts with relatively more deposits and assets should be more carefully assessed. In addition, if the bank at any time is informed of suspicious information about the previous information, further due diligence will be appropriate. Identifying funds and monitoring banks operating private banking accounts often get significant information about their clients, including the purpose for which customers set up private bank accounts. This information can establish a base line for account activity that will allow the bank to better detect suspicious activity and assess situations that require additional verification related to the source of funds. Banks are not expected, in the course of ordinary business, to verify the origin of each deposit placed in each private bank account. However, banks should monitor deposits and transactions as necessary to ensure that the activity is consistent with the information the bank has received about the client's funds and for the stated purpose and intended to use the account. Such monitoring will facilitate the identification of accounts that warrant additional supervision. Increased supervision of private bank accounts for senior foreign political figures For the purposes of private bank accounts under 31 CFR 1010.605 (p), regulations that define the term senior foreign political figures include one or more of the following: Current or former : Senior officials in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not). Senior of a major foreign political party. Senior executive director of a foreign state-owned commercial enterprise. 133For the purposes of this definition, the term senior official or senior executive means an individual with considerable authority over the policy, operation or use of government-owned resources. A company, business or other organization has been founded by, or for the benefit of any such individual. An immediate family member (including spouse, parents, siblings, children, and parents and siblings of the spouse) of any such individual. A widely known and publicly known person (or indeed known by the banks concerned) is a close link of that individual. Senior foreign political figures as defined above are often referred to as political contact people or PEPs. Refer to the extended overview section, Political Contacter, page 290, for further guidance, especially with to the appraisal of accounts maintained for PEPs that do not meet the regulatory definition of private bank account specified in 31 CFR 1010.605 (m). For private bank accounts to which a senior foreign political character is a notified or beneficial owner, the bank's due diligence program must include enhanced oversight that is appropriately designed to detect and report transactions that may be related to proceeds from foreign corruption. The term proceeds from foreign corruption means any property or property acquired by, through or on behalf of a senior foreign political person through the appropriation, theft or opriation of public funds, illegal conversion of foreign government assets or through acts of bribery or extortion , and includes any other assets to which any such assets have been converted or converted. 134The addition of red flags relating to transactions that may involve proceeds from foreign corruption is listed in the Guidelines on Strengthening supervision of transactions that may be related to proceeds from official foreign corruption, issued by the U.S. Department of the Finance, Federal Reserve , FDIC, OCC, OTS and U.S. Department of State, January 2001. In cases when a bank submits a SAR in connection with a transaction that may involve proceeds from foreign corruption, FinCEN instructed banks to include the term foreign corruption in the SAR narrative. 135Refer to Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption, FIN-2008-G005, 17 April 2008. Increased oversight of private bank accounts for senior foreign political figures should be based on risk. Reasonable steps to implement enhanced monitoring may include advising on publicly available information relating to the client's country, contacting affiliates U.S. banks operate in the client's country to get additional information about the customer and the political environment, and conduct closer monitoring of the client's employment history and sources For example, transferring money from a government account to the personal account of a government official with signature authority over a government account may raise suspicions of bank political corruption. Additionally, if a bank considers the main news sources to show that a client may or may be involved in political corruption, the bank should consider the client's account for unusual activity. Identifying senior foreign political figures banks that are required to establish policies, procedures and controls includes reasonable steps to determine an individual's status as a senior foreign political person. The procedure should require information relating to employment and other sources of income, and the bank should seek information directly from customers about the status of possible senior foreign political figures. The Bank should also examine references, if appropriate, to determine whether the individual holds or has previously held a senior political position or may be a close link of a senior foreign political person. In addition, the bank should make reasonable efforts to review public sources of information relating to customers. Banks applying reasonable due diligence procedures under 31 CFR 1010.620 may not be able to identify in any case individuals who qualify as senior foreign political figures, and especially their close relatives, and therefore cannot apply enhanced supervision to all such accounts. If the bank's due diligence program is properly designed to make this decision and the bank manages it effectively, then the bank can often detect, report and take appropriate action when suspicion of money laundering occurs on these accounts, even in cases where the bank is unable to identify the account owner as a political person high-level foreign countries ensure increased supervision. Special Procedures When due diligence cannot be carried out the bank's due diligence policy, procedures, and controls established under 31 CFR 1010.620(a) must include special procedures when proper due diligence cannot be carried out. These special procedures must include when the bank should: Refuse to open an account. Suspension of trading activity. File sar. Close the account. Page 11 Goals. Assess whether the bank complies with regulatory and regulatory requirements to implement policies, procedures, and controls to detect and report money laundering and suspicious activity through private bank accounts established, managed, or maintained for non-Americans. You. Refer to the extension of the manual for discussing and examining procedures related to the specific money laundering risk associated with private banking. 1. Determine whether the bank provides a private bank account as defined by the private bank account. Personal bank account means account (or any combination of accounts) at a financial institutions covered by regulations that meet all three criteria: Minimum total deposit requirements of funds or other assets not less than $1,000,000 (31 CFR 1010,605 (m) (1)). Founded on behalf of or for the benefit of one or more non-Americans. who is the direct or beneficial owner of the account (31 CFR 1010.605 (m) (2)). Specified, or managed or managed by all or part, a bank officer, employee or agent acts as a liaison between the bank and the direct or beneficial owner of the account (31 CFR 1010.605 (m) (3)). The final rules reflect the definition of the law found in the U.S. PATRIOT Act. If an account meets the last two criteria in the definition of a private bank account as described above, but the organization does not require a minimum balance of $1,000,000, then the account does not qualify as a private bank account under this rule. However, the account is subject to the risk-based internal controls and due diligence measures present in the organization's general BSA/AML compliance program.136Refer for extensive vesance procedures, Private Bank and Political Contacters (PEPs), pages 278 and 294, respectively, for further guidance. 2. Determine whether the bank has implemented due diligence policies, procedures and controls on private bank accounts established, maintained, managed or managed in the United States by a non-U.S. bank. You. Determine whether policies, procedures and controls are appropriately designed to detect and report any money laundering or suspected activity carried out through or in connection with any private bank account. 3. Review the bank's policies, procedures and controls to assess whether the bank's due diligence program includes reasonable steps to: Identify the name owner and the benefits of a private bank account (31 CFR 1010.620 (b) (1)). Determine whether any anonymous or beneficial owner of a private bank account is a senior foreign political person (31 CFR 1010.620(b) (2)). Identify the source(s) of deposits to the private bank account and the purpose and intended use of the private bank account for non-Americans. (31 CFR 1010.620(b)(3)). Review the activity of the account to ensure that it is consistent with the information obtained about the client's funds and for the stated purpose and intended use of the account, as necessary, to protect against money laundering and to report any known or suspicious money laundering activities carried out, from or through private bank accounts to non-Americans. (31 CFR 1010.620(b)(4)). 4. Review the bank's policies, procedures and controls to carry out advanced monitoring to assess whether they are appropriately designed to detect and report transactions that may be related to the proceeds from foreign corruption137 The term proceeds from foreign corruption means any property or or acquired by, through, or on behalf of a senior foreign political person through appropriation, theft, or the illegal realm of public funds, the illegal conversion of property by a foreign government, or through acts of bribery or extortion, and will include any other assets to which such assets have been converted or converted (31 CFR 1010,620 (c) (2). which a senior foreign political character138The last rule defines a senior foreign political person such as: a current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government, whether or not they are or have been elected as officials; a senior official of a major foreign political party; and a senior executive of a foreign state-owned commercial enterprise. This definition also includes a company, business, or other organization formed for or for the benefit of such an individual. Senior executives are individuals with considerable authority over policies, activities or use of government-owned resources. Also included in the definition of a senior foreign political official is immediate family members of individuals and those widely known and publicly known (or indeed known) close relatives of a senior foreign political person. is a nameless or beneficial owner (31 CFR 1010.620 (c) (1)). Check trades 5. On the basis of risk assessment, pre-inspection reports, and review of the bank's audit results, select a customer profile form to determine if the bank has identified the name and benefit owner, and the source of deposits to private bank accounts for non-U.S. private bank accounts. You. The selected form is as follows: Whether the bank's procedures comply with internal policies and regulatory requirements. Whether the bank has followed its procedures manages the risk assessment of private bank accounts for non-U.S. banks. You. Whether the bank implements increased oversight of private bank accounts to which senior foreign political figures are anonymous or beneficial owners, in accordance with policies, regulatory guidelines and regulatory requirements. 6. On the basis of complete inspection procedures, including transaction inspection, a conclusion on the possibility of policies, procedures and procedures to meet the regulatory requirements related to private banking due diligence programs. 7. On the basis of previous conclusions and risks related to the bank's activities in this field, conduct extensive inspection procedures, if necessary. Page 12 Goals. Assess the bank's compliance with regulatory and regulatory requirements for special measures enacted under section 311 of the US PATRIOT Act. Section 311 of the U.S. PATRIOT Act added 31 USC 5318A to the BSA, to allow the Minister of Finance to request domestic financial institutions and domestic financial institutions to take a number of special measures against foreign countries foreign financial institutions, international transaction classes, or account types of major money laundering concerns. Section 311 provides the Finance Minister with a range of options that can be adjusted to target specific concerns about money laundering and terrorist funding. Section 311 is implemented through various orders and regulations integrated into 31 CFR Chapter X.139Notices of the proposed rulemaking and the final rules that accompany the identification of major money laundering concerns, and impose a special measure(s) under section 311 of the US PATRIOT Act that is on theFinCEN website. As provided for in section 311, certain special measures may be applied by an order without notice and public comment, but such orders must be limited in time and must be issued in accordance with the Proposed Rules Notice. Section 311 establishes a process for the Secretary of The Finance to follow, and determines which federal agencies to consult before the Secretary of The Finance can conclude that an authority, financial institutions, transaction class, or account type are the main money laundering concerns. The Act also provides similar procedures, including elements and consulting requirements, to select specific special measures that are imposed on jurisdiction, financial institutions, type of transaction or type of account with major money laundering concerns. It is important to note that, while a legal area, financial institutions, transaction class or account type may be assigned on the main money laundering concern in an order issued in connection with the Proposed Rules Notice, special measures with an unlimited term can only be applied by a final rule issued after when notifying and opportunity to comment. Special types of measures The following five special measures can be applied, individually, generally or in any combination: Record and report certain financial transactions According to the first special measure, banks may be required to maintain records or file reports , or both, in relation to the total number of transactions or specific details of each transaction involving jurisdiction, financial institutions, transaction class or account type is the main money laundering concern. This Act contains minimum information requirements for these records and reports and allows the Minister of Finance to impose additional information requests. Information relating to beneficial ownership According to the second special measure, banks may be required to take reasonable and feasible steps, at the decision of the Secretary of The Treasury, to get and retain information relating to the beneficial ownership of any account opened or maintained in the United States by a foreigner (a foreigner foreign organizations with shares must comply with the requirements of publicly reported or listed and traded on a managed exchange or transaction or representatives of such foreigners, which are related to the authority, financial institutions, type of transaction or type of account related to primary money laundering. Information relating to certain accounts payable through accounts Under the third special measure, banks that open or maintain accounts payable through accounts in the United States relating to jurisdiction, financial institutions, transaction classes, or account types with major money laundering concerns may be required (i) to identify each client (and representative) permitted to use account application or whose transactions are routed through the account and (ii) to get information about each client (and representative) is significantly comparable to what the bank has in the normal course of business for its clients residing in the United States.140Refer to extend the overview section , Payable Through Accounts, page 194, for further instructions. Information relating to certain agency accounts by the fourth special measure, banks that open or maintain agency accounts in the United States in connection with jurisdiction, financial institutions, transaction class or type of account with primary money laundering concerns may be required: (i) identify each client (and representative) authorized to use the account or have transactions transferred through the account; and (ii) get information about each client (and representative) that is significantly comparable to a U.S. hosting organization that has been in normal business process for customers residing in the United States.141Refer to overview core sections, Foreign Correspondents account recordkeeping, reporting and due diligence , page 111, and extended overview section, Agent Account (Foreign), page 177, for further instructions. Prohibited or conditional on opening or maintaining certain agents or payable through accounts Under the fifth, and strongest measure, in particular, banks may be prohibited from opening or maintaining in the United States any agent account or payable through the account for, or on behalf of , a foreign financial institutions if the account involves an authority, financial institutions, transaction class, or type of account that is the main money laundering concern. The application of this measure may prohibit U.S. banks from establishing, maintaining, managing or managing in the United States an agent or paying through an account or on behalf of any financial institutions from a particular foreign legal area. This measure can also be applied to specific foreign financial institutions and their subsidiaries. Regulations that implement these bans may require banks to review their account records to determine if they do not maintain accounts directly for, or on behalf of those bodies. In addition to direct prohibition, banks also suffered: Prohibited from intentionally providing indirect access to specific bodies through their other banking relationships. It is mandatory to notify the agent account owner that they are not provided to the specific agent with access to the account maintained at the U.S. bank. Reasonable steps must be taken to determine any indirect use of his account by a particular agent. Special commands and regulations guiding special measures to take specific special measures taken under section 311 of the U.S. PATRIOT Act are non-static; they can be issued or cancelled from time to time as the Minister of Finance determines that the authority of the subject, organization, transaction class or type of account is no longer a major money laundering concern. In addition, special measures that apply to a legal area, organization, transaction class, or account type may differ from those imposed in other situations. Examiners should also note that an order or rule imposing a special measure may establish an appraisal standard that banks must apply to comply with specific special measures. Accordingly, this manual does not detail specific special final measures, because any such list can quickly become date. Examiners considering compliance with this section should visit the FinCEN website for current information on final special measures. Examiners should only check for special measures that are final, and should not consider banks for special measures proposed. Page 13 Goals. Assess the bank's compliance with regulatory and regulatory requirements for special measures enacted under section 311 of the U.S. PATRIOT Act. 1. Determine the extent of international banking activities of banks and foreign legal regions in which banks conduct transactions and operations, with particular emphasis on foreign agent banks and account payments. 2. If possible, determine whether the bank has established policies, procedures and procedures to meet the specific special measures applied by FinCEN to its operations. Assess the completeity of account detection policies, procedures and procedures or transactions with legal areas, financial institutions or transactions subject to special final measures. 3. Identify, through discussions with management and review of bank documents, whether the bank has taken action in response to special final measures. Check trades 4. Identify all special final measures issued by FinCEN under section 311 applicable to the bank (refer to the FinCEN website). 5. For any of the first four types of special measures, determine whether the bank obtained, recorded, or reported the information as required by each particular special measure. 6. For the fifth special measure (prohibition), determine whether the bank complies with the prohibitions restrictions as required by each specific special measure, and to comply with any required by special measures. 7. When necessary, the bank's MIS search and other appropriate records for accounts or transactions with legal areas, financial institutions or transactions are subject to special final measures. 8. On the basis of complete inspection procedures, including transaction inspection, a conclusion on the possibility of policies, procedures and procedures to meet the regulatory requirements related to special measures. Page 14 Goals. Assess the bank's compliance with regulatory and regulatory requirements for foreign bank and financial account reports. Each person142As is defined in 31 CFR 1010,100 (mm), the term person means an individual, a corporation, a partnership, a trust or real estate, a holding company, an association, a corporation, a joint venture or other uninsted organization or group, an Indian Tribe (as that term is defined in the Indian Gaming Regulations Act) , and all recognizable bodies are legal personalities. The IRS guidelines add that the term American includes U.S. citizens; U.S. residents; organizations, including but not limited to, corporations, code companies or limited liability companies, established or organized in the United States or under U.S. law; trusts or real estate formed under U.S. law. Refer to the IRS FBAR Reference Guide. See also BSA Electronic Filing Requirements for Offshore Bank And Financial Account Reports (Form FinCEN 114) June 2014 Release Date (v1.3) Effective October 2013 for 2013 or previous filing requirements. (including banks) subject to U.S. jurisdiction with financial interests or signatures or other jurisdiction over banks, securities or any other offshore financial accounts must file electronic reports of Offshore Bank and Financial Accounts (FBAR) through the BSA Electronic Filing System if the total value of these financial accounts exceed $10,000 at any time in the calendar year.14331 CFR 1010350. The term financial account usually includes, among other things, accounts in which the asset is held in a traded fund and the account holder holds the equity interest rate in the fund, (e.g. a mutual fund), as well as a debit card and prepaid card account. A bank must submit an FBAR on its own account that meets this definition; in addition, the bank may be obliged to submit these forms to customer accounts in which the bank has financial interest or is signed or otherwise authorized. FBAR must be filed on or before June 30 of each calendar year for offshore financial accounts where the total value exceeds $10,000 at any time in the previous calendar year. FinCEN has issued a final rule effective from March 28, 2011 regarding reports of offshore financial accounts.144Refer to Fed. Reg. 10234 (February 24, 2011). FinCEN then announces an extension of the time for certain FBAR applications due to ongoing questions regarding the application and its application for authorized individuals signed on but no financial interest in some types of accounts. On February 14, 2012, FinCEN issued Notice 2012-1 to extend the filing date for some individuals with signature authority but no financial interest in one or more offshore financial accounts. The FBAR filing deadline for Americans with only the authority to sign on (but not financially) a foreign financial account has been extended to June 30, 2015. Page 15 Goals. Assess the bank's compliance with regulatory and regulatory requirements for foreign bank and financial account reports. 1. Determine whether the bank is interested in finance, signatures or other jurisdiction over bank accounts, securities or other offshore financial accounts, as well as whether the bank must submit a Foreign Bank report and Financial Account (FBAR) to the client's account, including the trust account , in which the bank has financial interest or is signed or otherwise authorized. 2. If possible, consider the bank's policies, procedures and annual reporting process. Check transaction 3. On the basis of risk assessment, pre-inspection report and review of the bank's audit results, select an account form to determine if the bank has completed, submitted and retained copies of FBAR forms appropriately. 4. On the basis of complete inspection procedures, including transaction inspection, form a conclusion about the possibilities of policies, procedures, and processes to meet regulatory requirements related to FBARs. Page 16 Goals. Assess the

bank's compliance with regulatory and regulatory requirements for reporting international shipments of currency or monetary instruments. Each person145As is defined in 31 CFR 1010,100 (mm), the term person means an individual, a corporation, a partnership, a trust or real estate, a holding company, an association, a corporation, a joint venture or other uninsted organization or group, an Indian Tribe (as that term is defined in the Indian Gaming Regulations Act) , and all recognizable bodies are legal personalities. (including a bank) physical shipping, mail or currency shipping or monetary instrument in excess of $10,000 at the same time out of or into the United States (and each person who causes such shipping, mailing or shipment) must file a Currency Shipping Report or International Monetary Instrument (CMIR).146The obligation to file CMIR is based solely on the carrier , mail, ships or received, or causes or attempts to transport, mail, ship, or receive. No other person is obliged to file CMIR. So if a customer enters the bank and claims that they have received or shipped currency in an additional amount in excess of $10,000 from a place outside the United States and wishes to deposit the currency into his or her account, the bank is under no to file a CMIR on behalf of the client (see FIN-1998-R002 formerly known as Treasury Administrative Judgment 88-2). Also refer to the CMIR guidelines for popular currency carriers, including armored vehicle service, FIN-2014-G002, August 1, 2014. A CMIR must be filed with the appropriate Customs and Border Service or with the Customs commissioner at the time of entry or departure from the United States. When a person receives currency or monetary instrument in an amount in excess of $10,000 at a time that has been shipped from anywhere outside the United States, a CMIR must be filed with the appropriate customs department and border protection officer or with the Customs commissioner within 15 days of receiving the instrument (unless a report has been filed). The report will be completed by or on behalf of the person requesting the transfer of currency or currency instruments. However, banks are not required to report these items on CMIR if they are mailed or shipped by postal service or by ordinary carrier.147 Conversely, the bank is required to submit CMIR to report currency shipments or monetary instruments to foreign offices when such shipments are made directly by the bank members, such as currency shipments processed by bank employees by means owned by the bank. In addition, a commercial bank or trust company held under the laws of any state or of the United States is not required to report shipments on the set of currency or monetary instruments if they are shipped to or received from an established customer maintaining a deposit relationship with the bank and if the bank concludes reasonable no. money does not exceed what is commensurate with the usual behavior of the business, industry, or occupation of the relevant customer. Regardless of whether the CMIR application waiver applies, banks are not exempt from other monitoring and reporting obligations under the BSA. Banks must report receiving or disbursing currencies in excess of $10,000 on the Currency Transactions Report (CTR) depending on the waiver at 31 CFR 1020315. Banks must also monitor and report suspicious activity. Management should implement the policies, procedures and procedures applicable to CMIR filing. Management should consider the international transportation of monetary and monetary instruments and determine whether customer activity is normal and routine for this type of business. Otherwise, sar should be considered. Page 17 Goals. Assess the bank's compliance with regulatory and regulatory requirements for reporting international shipments of currency or monetary instruments. 1. Determine whether the bank has (or has caused) the currency shipped, mailed or shipped or other monetary instruments in excess of $10,000, at the same time, out of the United States, or whether the bank has received currency or other monetary instruments in excess of $10,000, at the same time , has been shipping, mailing or shipping into the United States. 2. If possible, consider the bank's policies, procedures and procedures for filing a Currency Shipping Report or International Monetary Instrument (CMIR) for each currency shipment or other monetary instrument that exceeds $10,000 out of or into the United States (except for shipments sent through the postal service , the usual carrier or another exception from the applicable CMIR report). Check transaction 3. On the basis of risk assessment, pre-inspection report and review of the bank's audit results, select a transaction form made after the previous inspection to determine if the bank has completed, submitted and retained copies of CMIRs appropriately. 4. On the basis of complete inspection procedures, including transaction inspection, form a conclusion about the possibilities of policies, procedures, and processes to meet regulatory requirements related to CMIRs. 5. On the basis of previous conclusions and risks related to the operation of the bank in this field, conduct extensive inspection procedures, if necessary. Page 18 Goals. Assess the bank's Office of Foreign Assets Control (OFAC) compliance program based on the bank's risk to assess whether it is consistent with the bank's OFAC risk, taking into account the bank's products, services, customers, bodies, transactions and geographic location. OFAC is an office of the U.S. Department of the United States that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security objectives against targeted individuals and organizations such as foreign countries, regimes, terrorists, international drug traffickers, and those engaged in certain activities such as weapons of mass destruction or transnational organized crime. OFAC operates under the President's national and war time emergency powers, as well as various agencies granted by specific laws, to impose controls on transactions and freeze assets under U.S. jurisdiction. OFAC has been tasked by the Secretary of the Finance to develop, enact, and administer U.S. sanctions programs. 148Trading With the Enemy Act (TWEA), 50 USC App 1-44; International Emergency Economic Powers Act (IEEPA), 50 USC 1701 et seq.; Effective Counterterrorism and Death Penalty Act (AEDPA), 8 USC 1189, 18 USC 2339B; United Nations Participation Act (UNPA), 22 USC 287c; Cuban Democracy Act (CDA), 22 USC 6001–10; Cuban Democratic Freedom and Solidarity Act (Libertad Act), 22 USC 6021–91; Clean Diamond Trade Act, pub. L. No. 108-19; Foreign Drug Lords Designing Act (Kingpin Act), 21 USC 1901-1908, 8 USC 1182; Burma Freedom and Democracy Act 2003, Pub. L. No. 108–61, 117 Stat. 864 (2003); Foreign activities, export finance and related programs Appropriations Act, Sec. 570 of Pub. L. No. 104-208, 110 Stat. 3009-116 (1997); Punitive Act Pub. L. No. Not. 104 Statistics 2047-55 (1990); International Security and Development Cooperation Act, 22 USC 2349 aa8–9; Trade Sanctions Reform and Strengthening Act 2000, Title IX, Pub. L. No. 106-387 (October 28, 2000). Many of these sanctions are based on the duties of the United Nations and other international mandates; therefore, they are multilateral in scope, and involve close cooperation with allied governments. Other sanctions are reserved for U.S. national security interests. On 9 November 2009, OFAC issued a final rule called the Economic Sanctions Enforcement Guidelines to provide guidance to those who comply with its regulations. The document explains the procedures by which OFAC complies in determining appropriate enforcement responses to clear violations of its regulations. Some enforcement responses can result in the enacting of a civil penalty that, depending on the sanctioning program affected, can be up to $250,000 per violation or double the amount of a transaction, which, under any larger condition. The guidelines outline the various factors that OFAC takes into account when making enforcement decisions, including the completeness of a compliance program put in place within an organisation to ensure compliance with OFAC regulations. 149Refer to 73 Fed. Reg. 57593 (November 9, 2009) for more information (also available on ofac's website). All Americans, 150 All Americans must comply with OFAC regulations, including all U.S. citizens and permanent residents no matter where they are, all people and agencies within the United States, all U.S. a united states and their foreign affiliates. In the event that certain programs, such as those related to Cuba and North Korea, foreign subsidiaries owned or controlled by U.S. companies must also comply. Some programs also require foreigners to own goods of U.S. origin to comply. including U.S. banks, bank holding companies, and non-bank subsidiaries, subject to OFAC regulations. 151So more information is provided in foreign asset control regulations to the financial community, which is available on ofac's website. Federal banking authorities evaluate OFAC compliance programs to ensure that all banks subject to their supervision comply with sanctions. 15231 CFR Chapter V. Unlike BSA, the laws and regulations enacted by OFAC not only apply to U.S. banks, branches, domestic agencies and international banking facilities, but also to their foreign affiliates, and often overseas offices and subsidiaries. OFAC encourages banks to take a risk-based approach to designing and implementing the OFAC compliance program. Generally, the regulations administered by OFAC require banks to do the following: Block accounts and other assets of organizations and individuals are specified. Prohibit or deny uns permitd commercial and financial transactions with specified countries, organizations and individuals. Transactions blocked by U.S. law require assets and accounts of a country, organization, or individual specified by OFAC are blocked when such property is located in the United States, held by U.S. individuals or organizations, or owned or controlled by U.S. individuals or organizations. For example, if the money transfer is coming from abroad and is being transferred through a U.S. bank to a foreign bank and there is a party assigned by OFAC to participate in the transaction, it must be blocked. The definition of assets and assets is broad and is specifically defined in each sanctioning program. Assets and assets include any direct, indirect, current, forward or backup value (including all types of banking transactions). Banks must block transactions: By or on behalf of a blocked individual or organization; Is to or go through a blocked body; or Is related to a transaction in which a blocked person or organization is interested. For example, if a U.S. bank receives instructions to make a money transfer payment that falls into one of these categories, it must make a payment order and place the funds in a blocked account. Blocked account 153A is an account with a segregated interest rate (at a commercially reasonable rate), holding the client's assets until the target is delisted, the sanctions program is canceled or the client has an OFAC license that allows the issuance of assets. A payment order cannot be cancelled or amended after receiving a U.S. bank without permission from OFAC. Prohibited transactions In some cases, a basic transaction may be prohibited, but there is no blockable interest in the transaction (i.e. the transaction should not be accepted, but there is no OFAC requirement to block the asset). In these cases, the transaction is simply rejected, (i.e., not processed). For example, the Sudanese Sanctions Regulation prohibits transactions that support commercial activities in Sudan. Therefore, a U.S. bank will have to refuse to transfer money between two companies, not a SpecialLy Specified Citizen or Blocked Person (SDN), in connection with the export to a company in Sudan nor the SDN. Because the Sudanese sanctions regulations will only require blocking transactions with the Sudanese Government or SDN, there will be no deterrent interest in funds between the two companies. However, because the transactions would constitute the export of services to Sudan, which is prohibited, the U.S. bank could not process the transaction and simply rejected the transaction. It is important to note that the OFAC regime prohibits certain countries, bodies and individuals as separate and distinct from those in the BSA's CIP regulations (31 CFR 1020220 (a) (4)) that require banks to compare new accounts with a list of known or suspected terrorist organizations of the government over a period of time reasonable time after the account is opened. OFAC is not specified on the government list for the purposes of the CIP rule. Refer to the core overview, Customer Identification Program, page 47, for further instructions. However, OFAC's requirements come from other laws not limited to terrorism and OFAC sanctions apply to transactions, in addition to account relationships. Ofac License OFAC has the authority, through a licensing process, to allow certain transactions which would otherwise be prohibited under its regulations. OFAC may issue a license to engage in another prohibited transaction when it determines that the transaction does not undermine U.S. policy objectives under a specific sanctions program, or is justified by U.S. national security or foreign policy objectives. OFAC may also issue general licenses, allowing transaction categories, such as allowing reasonable service charges on blocked accounts, without case-by-case permission from OFAC. These licenses can be found in the provisions for each sanctioning program (31 CFR, Chapter V (Regulation)) and can be accessed from ofac's website. Before processing transactions that can be covered under a general license, banks should verify that such transactions meet the relevant criteria of the general license. 154License information for a specific sanctioning program is available on ofac's website or by contacting ofac's licensing area at (202) 622-2480. Specific licenses are granted on a case-by-case basis. 155 Applications for a specific license may be submitted online from ofac's website, or written to: Licensing Division, Office of Foreign Assets Control, 1500 Pennsylvania Avenue, NW, Washington, DC 20220. A specific license is a written license issued by OFAC that allows a specific transaction or set of transactions that are usually limited for a certain period of time. To receive a specific license, the person or organization wishing to make the transaction must apply to OFAC. If the transaction is in accordance with OFAC's internal licensing policies and U.S. foreign policy objectives, the license is usually granted. If the bank's customer claims to have a specific license, the bank should verify that the transaction is in accordance with the terms and conditions of the license (including the effective date of the license), and may wish to have and retain a copy of the license for record keeping purposes. Banks reporting ofac must report all blocks to OFAC within 10 business days of occurring and annually before September 30 in relation to blocked assets (as of June 30). 156The annual reports will be filed on form TD F 90-22.50. When assets or funds are blocked, they are placed in a separate blocked account. Prohibited transactions must also be reported to OFAC within 10 business days of the date of the incident. 157 Reports, procedures and penalty regulations, 31 CFR Part 501. Banks must keep a complete record and the transaction is rejected at least five years from the transaction date. For blocked assets (including blocked transactions), records must be maintained for the duration of the asset being blocked and for five years after the date the asset is unblocked. Additional information relating to OFAC regulations, such as the Sanctions Program and national Summary promotional materials; SDN and other lists, including individuals and individuals; recent OFAC action; faqs, which can be found on ofac's website. 158 This information is available on ofac's website, or by contacting OFAC's hotline at (202) 622-2490 or toll-free at (800) 540-6322. OFAC Compliance Program Although not required by specific regulations, it is a matter of reasonable banking practice and to minimize risks of non-compliance with OFAC requirements, banks should establish and maintain an effective, written OFAC compliance program commensurate with their OFAC risk profile (product-based) , services, customers and geographical location). The program should identify higher risk areas, provide appropriate internal controls for screening and reporting, establish independent testing of compliance, appoint bank employees or employees responsible for COMPLIANCE with OFAC, and create appropriate employee training programs in all relevant sectors of the bank. OFAC Risk Assessment A fundamental element of ofac compliance programme is the bank's assessment of specific product lines, customer base and the nature of transactions and identification of areas of higher risk to potential OFAC sancations risk. The initial identification of the customer with higher risk for ofac purposes can be carried out as part of the bank's CIP and CDD procedures. As OFAC sanctions have access to virtually all areas of their operations, banks should consider all types of transactions, products and services when conducting risk assessments and establish appropriate policies, procedures and procedures. Effective risk assessment must be a combination of many factors (as described in more detail below) and depending on the circumstances, certain factors may be weighed over other factors. Another consideration for risk assessment is the account and trading parties. The new account should be compared to the OFAC list before it is opened or immediately afterwards. However, the scope to which the bank consists of non-account parties (e.g. beneficiaries, premises, premises, agents, beneficial owners, nominee shareholders, directors, signees and attorneys' powers) during the initial OFAC review during the account opening process and during the next database review of existing accounts, will depend on the bank's risk profile and available technology. Based on the bank's OFAC risk profile for each available sector and technology, the bank should policies, procedures and procedures for reviewing transactions and transactions (e.g., bank issue, payment recipient, confirmer, or jurisdiction.) Currently, OFAC provides guidance on cheque-based traders. The guidelines state that if a bank knows or has reason to know that a cheque transaction is the goal of OFAC, the bank's processing of transactions will result in the bank being liable, especially transactions processed individually in a higher risk area. For example, if a bank knows or has reason to know that cheque transactions involve a party or country banned by OFAC, OFAC will expect timely identification and appropriate action. When assessing the level of risk, a bank should make a judgment and take into account all risk indicators. While not an complete list, examples of products, services, customers, and geographic locations that may carry a higher level of OFAC risk include: International Money Transfers. Non-resident foreigner account. Foreign client accounts. Cross-border automatic clearing house (ACH) transactions. Trade letters of credit and other commercially funded products. Electronic banking transactions. Offshore agent bank account. Payable via account. Centrally account. International private bank. Overseas branches or subsidiaries. Appendix M (Risk Number - OFAC Procedure) provides guidance to assessing the OFAC risk assessments faced by the bank. Risk assessment can be used to assist examiners in determining the scope of the OFAC exam. Additional compliance risk information is posted by OFAC on its website in the FAQ. 159 This guide is available on the Ofac Website. Once the bank has identified areas with higher OFAC risks, the bank should develop appropriate policies, procedures and procedures to address the risks involved. Banks can adjust these policies, procedures and processes according to the specific nature of a product line or business product line. Furthermore, banks are encouraged to periodically re-assess their OFAC risks. Internal Controls An effective OFAC compliance program should include internal controls to identify suspicious accounts and transactions, as well as reporting blocked and rejected transactions to OFAC. Internal controls should include the following factors: Identify and review suspicious transactions. The bank's policies, procedures and procedures should address how the bank will identify and review transactions and accounts for possible OFAC breaches, whether done manually, through intervention software or a combination of both. For screening purposes, the bank should clearly define its criteria for comparing the names provided in the OFAC list with the names on the bank's records or on transactions and to identify transactions or accounts related to the sanctioned countries. The bank's policies, procedures and procedures should also address how it will determine whether the OFAC valid matches or mismatched. 160 Due diligence steps to determine a valid match provided in Use on the ofac website. A large volume of false hits may show the need to review the bank's intervention program. The screening criteria used by banks to identify name variations and spelling errors must be based on the level of OFAC risk associated with a particular product or type of transaction. For example, in a higher risk area with high transaction volume, the bank's intervention software will be able to identify sources of close name origin for review. The SDN list tries to provide the originating name; however, the list may not include all sources of origin. More complex intervention software can catch variations of the name of the SDN that are not included in the SDN list. Banks with lower OFAC risks and those with low transaction volumes may decide to filter OFAC compliance manually. The decision to use the intervention software and its sensitivity must be based on the bank's assessment of its risks and trading volume. When determining how often OFAC checks and filtering criteria are used (e.g., name origin), banks should consider the possibility of a breach and available technology. In addition, banks should periodically re-evaluate their OFAC filtration systems. For example, if a bank determines a name origin of an OFAC target, then OFAC shows that the bank adds names to its filtration process. The new account should be compared to the OFAC list before it is opened or immediately afterwards (e.g. during nightly processing). Banks that perform OFAC checks after opening an account should have procedures in place to prevent transactions, other than the original deposit, from occurring until the OFAC check is completed. Prohibited transactions made before completing an OFAC inspection may be subject to possible enforcement action. In addition, banks need policies, procedures and procedures to check existing customers when ofac listings are added or changed. The frequency of the review must be based on the bank's OFAC risk. For example, banks with lower OFAC risk levels may periodically (e.g., weekly, monthly, or quarterly) compare customer base with OFAC listings. Transactions such as money transfers, letters of credit and non-customer transactions must be checked for OFAC listings before being made. As ofac's policies, procedures and procedures evolve, the bank should remember that OFAC considers continuing the operation of an account or processing transactions after its alliation, along with the completeness of the bank's OFAC compliance program, as a factor in determining the appropriate enforcement response to a clear violation of OFAC regulations. 161Refer to 74 Fed. Reg. 57593 (November 9, 2009), Guidelines for the Enforcement of Economic Sanctions. More information is available on ofac's website. The Bank should maintain its OFAC audit documents on new accounts, existing customer facilities and If a bank uses a third party, such as an agent or service provider, to perform OFAC checks on its behalf, as with any other liability performed by a third party, the bank is ultimately responsible for complying with such third-party requirements with ofac requirements. Therefore, banks need to have a written agreement and establish controls and a full review of procedures for such relationships. Update the OFAC list. The bank's OFAC compliance program must include policies, procedures and procedures to promptly update the list of sanctioned countries and blocked individuals and agencies and individuals, and disseminate such information throughout the bank's domestic operations and offices , overseas branches and, in the case of Iran and Cuba, foreign subsidiaries. This will include ensuring that any manually updated software interventions are completed in a timely manner. Screening of automatic clearing house (ACH) transactions. ACH transactions may involve people or parties subject to ofac-administered sanctions programs. Refer to the extended overview, Automatic Home Clearing Transaction, page 216, for further instructions. OFAC clarified the application of OFAC rules for domestic and cross-border ACH transactions and provided more detailed guidance on international ACH transactions. 162Refer to Guidance to National Automated Clearing House Association (NACHA) on cross-border ACH transactions. For domestic ACH transactions, the Originating Deposition Finance Organization (ODFI) is responsible for verifying that the Originator is not a blocked party and making a goodwill effort to determine that the Originator does not transmit blocked funds. The same financial institutions (RDFI) are responsible for verifying that the recipient is not a blocked party. In this way, ODFI and RDFI are relying on each other to comply with OFAC regulations. If an ODFI receives domestic ACH transactions that its clients have batched, ODFI is not responsible for unbatching transactions to ensure that no transactions violate OFAC regulations. If an ODFI unbatches an initial file received from the originater to process on-us transactions, ODFI is responsible for OFAC compliance for on-us transactions because it acts as both ODFI and RDFI for transactions. ODFIs operating in this capacity should have known their customers for the purposes of OFAC and other regulatory requirements. For the remaining transactions that have not been operated on the file are not on-us, as well as situations where banks processing ACH records have not been operated on for reasons other than the elimination of transactions in the United States, banks should determine the extent of their OFAC risks and develop policies appropriate procedures and procedures for addressing the risks involved. Such policies may involve screening individual unoperative ACH records. in doing so, banks may with third-party service providers should evaluate those relationships and their related ACH transactions to determine the bank's OFAC risk level and develop appropriate policies, procedures and procedures to mitigate that risk. For cross-border screening, OFAC obligations are similar but somewhat more stringent for international ACH transactions (IAT). In the case of domestic IATs, and regardless of whether the OFAC flag in the IAT is established, an RDFI is responsible for complying with the OFAC sanctions program. However, for away IATs, ODFI cannot rely on OFAC screening by RDFI outside the United States. In these situations, ODFI must perform painstaking enhancements to ensure that illegal transactions are not processed. Due diligence for an IAT at home or abroad may include screening the parties to a transaction, as well as reviewing the details of the payment field information for an indication of a violation of sanctions, investigating the result hits, if any, and ultimately blocking or rejecting the transaction, as appropriate. Refer to the extended overview, Automatic Home Clearing Transaction, page 216, for further instructions. Additional information about the types of retail payment systems (ACH payment systems) is available in the FFIEC Information Technology Inspection Handbook. 163Refer to the FFIEC Information Technology Examination Handbook's Retail Payment Systems booklet. In guidelines issued March 10, 2009, OFAC authorizes organizations in the United States when they are acting as an ODFI/Gateway Operator (GO) for domestic IAT debits to reject transactions that appear to involve interceptable assets or property interests. 164Refer to nacha site. Guidelines continue to say that to the fullest scope that an ODFI/GO domestic IAT debit screen for OFAC violations is possible before implementation and during such screening detects a potential OFAC violation, the suspected transaction is to be removed from the batch for further investigation. If ODFI/GO determines that the transaction appears to be in violation of ofac regulations, ODFI/GO should refuse to process the transfer. The procedure applies to commonly blocked transactions as well as transactions that are generally rejected for OFAC purposes based on the information in payment. Report. An OFAC compliance program should also include policies, procedures and procedures for handling items that are validly blocked or disapproved under various sanctions programs. When there is a question about the validity of the intervention, banks can contact OFAC by phone or electronic hotline for guidance. Most other items should be reported through regular channels within ten days of occurring. Policies, procedures and procedures should also address the management of blocked accounts. Banks are responsible for tracking the amount blocked, ownership of those funds, and the interest paid to those funds. Total amount blocked, must be reported to OFAC by September 30 each year (as of June 30). When a bank acquires or merges with another bank, both banks should consider the need to review and maintain such records and information. Banks no longer need to file SARs based solely on drug-related transactions or blocked terrorism, as long as the bank submits the necessary blocking report with OFAC. However, because blocking a report requires only limited information, if the bank owns additional information that is not included in the OFAC blocking report, a separate SAR should be submitted to FinCEN that includes that information. In addition, the bank should file a sar if the transaction itself will be considered suspicious in the event of a valid OFAC match. 165 Reference FinCEN Release Number 2004-02, Unitary Filing of Suspicious Activity and Blocking Reports, 69 Fed. Reg. 76847 (December 23, 2004). Maintain license information. OFAC recommends that banks consider maintaining a copy of the client's OFAC licence on file. This will allow the bank to verify whether the client has started a legal transaction. Banks should also know the expiration date on the OFAC licence. If it is unclear whether a particular transaction is authorized under the terms of the license, the bank should contact OFAC. Maintaining copies of ofac licenses will also be useful if another bank in the payment chain requires verification of the validity of the license. Copies of ofac licenses must be maintained for five years, after the most recent transaction is carried out under license. Independent testing Each bank should conduct an independent test of the OFAC compliance program conducted by internal auditors, external auditors, consultants or other qualified independent parties. For large banks, the frequency and area of independent testing should be based on known risks or perceptions of specific business sectors. For smaller banks, the audit must be in line with the bank's OFAC risk profile or based on cognitive risk. The person responsible for the inspection must conduct an objective and comprehensive review of OFAC's policies, procedures and procedures. The scope of the audit must be comprehensive enough to assess ofac compliance risks and assess the completeness of the OFAC compliance program. It is the individual responsible for requesting each bank to appoint a qualified individual(s) responsible for the day-to-day compliance of the OFAC compliance program, including changes or updates to various sanctions programs and reporting blocked or rejected transactions to OFAC and monitoring of blocked funds. This individual should have an appropriate level of knowledge about ofac regulations commensurate with the bank's OFAC risk profile. The Bank training should provide adequate training to all appropriate staff on its OFAC compliance programmes, processes and processes. The and the frequency of training must be consistent with the bank's OFAC risk profile and in line with the responsibilities of the staff. Page 19 19