

Office of Foreign Assets Control — Overview

Objective. *Assess the bank’s risk-based Office of Foreign Assets Control (OFAC) compliance program to evaluate whether it is appropriate for the bank’s OFAC risk, taking into consideration its products, services, customers, entities, transactions, and geographic locations.*

OFAC is an office of the U.S. Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted individuals and entities such as foreign countries, regimes, terrorists, international narcotics traffickers, and those engaged in certain activities such as the proliferation of weapons of mass destruction or transnational organized crime.

OFAC acts under Presidential wartime and national emergency powers, as well as various authorities granted by specific legislation, to impose controls on transactions and to freeze assets under U.S. jurisdiction. OFAC has been delegated responsibility by the Secretary of the Treasury for developing, promulgating, and administering U.S. sanctions programs.¹⁴⁸ Many of these sanctions are based on United Nations and other international mandates; therefore, they are multilateral in scope, and involve close cooperation with allied governments. Other sanctions are specific to the national security interests of the United States.

On November 9, 2009, OFAC issued a final rule entitled “Economic Sanctions Enforcement Guidelines” in order to provide guidance to persons subject to its regulations. The document explains the procedures that OFAC follows in determining the appropriate enforcement response to apparent violations of its regulations. Some enforcement responses may result in the issuance of a civil penalty that, depending on the sanctions program affected, may be as much as \$250,000 per violation or twice the amount of a transaction, whichever is greater. The Guidelines outline the various factors that OFAC takes into account when making enforcement determinations, including the adequacy of a compliance program in place within an institution to ensure compliance with OFAC regulations.¹⁴⁹

All U.S. persons,¹⁵⁰ including U.S. banks, bank holding companies, and nonbank subsidiaries, must comply with OFAC’s regulations.¹⁵¹ The federal banking agencies

¹⁴⁸ Trading With the Enemy Act (TWEA), 50 USC App 1-44; International Emergency Economic Powers Act (IEEPA), 50 USC 1701 *et seq.*; Antiterrorism and Effective 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; The Cuban Liberty and Democratic Solidarity Act (Libertad Act), 22 USC 6021–91; The Clean Diamonds Trade Act, Pub. L. No. 108-19; Foreign Narcotics Kingpin Designation Act (Kingpin Act), 21 USC 1901–1908, 8 USC 1182; Burmese Freedom and Democracy Act of 2003, Pub. L. No. 108–61, 117 Stat. 864 (2003); The Foreign Operations, Export Financing and Related Programs Appropriations Act, Sec 570 of Pub. L. No. 104-208, 110 Stat. 3009-116 (1997); The Iraqi Sanctions Act, Pub. L. No. 101-513, 104 Stat. 2047-55 (1990); The International Security and Development Cooperation Act, 22 USC 2349 aa8–9; The Trade Sanctions Reform and Export Enhancement Act of 2000, Title IX, Pub. L. No. 106-387 (October 28, 2000).

¹⁴⁹ Refer to 73 *Fed. Reg.* 57593 (November 9, 2009) for additional information (also available on the [OFAC Web site](#)).

¹⁵⁰ All U.S. persons must comply with OFAC regulations, including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, all U.S.

evaluate OFAC compliance programs to ensure that all banks subject to their supervision comply with the sanctions.¹⁵² Unlike the BSA, the laws and OFAC-issued regulations apply not only to U.S. banks, their domestic branches, agencies, and international banking facilities, but also to their foreign branches, and often overseas offices and subsidiaries. OFAC encourages banks to take a risk-based approach to designing and implementing an OFAC compliance program. In general, the regulations that OFAC administers require banks to do the following:

- Block accounts and other property of specified countries, entities, and individuals.
- Prohibit or reject unlicensed trade and financial transactions with specified countries, entities, and individuals.

Blocked Transactions

U.S. law requires that assets and accounts of an OFAC-specified country, entity, or individual be blocked when such property is located in the United States, is held by U.S. individuals or entities, or comes into the possession or control of U.S. individuals or entities. For example, if a funds transfer comes from offshore and is being routed through a U.S. bank to an offshore bank, and there is an OFAC-designated party to the transaction, it must be blocked. The definition of assets and property is broad and is specifically defined within each sanction program. Assets and property includes anything of direct, indirect, present, future, or contingent value (including all types of bank transactions). Banks must block transactions that:

- Are by or on behalf of a blocked individual or entity;
- Are to or go through a blocked entity; or
- Are in connection with a transaction in which a blocked individual or entity has an interest.

For example, if a U.S. bank receives instructions to make a funds transfer payment that falls into one of these categories, it must execute the payment order and place the funds into a blocked account.¹⁵³ A payment order cannot be canceled or amended after it is received by a U.S. bank in the absence of an authorization from OFAC.

incorporated entities and their foreign branches. In the case of certain programs, such as those regarding Cuba and North Korea, foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S. origin goods to comply.

¹⁵¹ Additional information is provided in *Foreign Assets Control Regulations for the Financial Community*, which is available on [the OFAC Web site](#).

¹⁵² 31 CFR Chapter V.

¹⁵³ A blocked account is a segregated interest-bearing account (at a commercially reasonable rate), which holds the customer's property until the target is delisted, the sanctions program is rescinded, or the customer obtains an OFAC license authorizing the release of the property.

Prohibited Transactions

In some cases, an underlying 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 assets). In these cases, the transaction is simply rejected, (i.e., not processed). For example, the Sudanese Sanctions Regulations prohibit transactions in support of commercial activities in Sudan. Therefore, a U.S. bank would have to reject a funds transfer between two companies, which are not Specially Designated Nationals or Blocked Persons (SDN), involving an export to a company in Sudan that also is not an SDN. Because the Sudanese Sanctions Regulations would only require blocking transactions with the Government of Sudan or an SDN, there would be no blockable interest in the funds between the two companies. However, because the transactions would constitute the exportation of services to Sudan, which is prohibited, the U.S. bank cannot process the transaction and would simply reject the transaction.

It is important to note that the OFAC regime specifying prohibitions against certain countries, entities, and individuals is separate and distinct from the provision within the BSA's CIP regulation (31 CFR 1020.220(a)(4)) that requires banks to compare new accounts against government lists of known or suspected terrorists or terrorist organizations within a reasonable period of time after the account is opened. OFAC lists have not been designated government lists for purposes of the CIP rule. Refer to the core overview section, "Customer Identification Program," page 47, for further guidance. However, OFAC's requirements stem from other statutes not limited to terrorism, and OFAC sanctions apply to transactions, in addition to account relationships.

OFAC Licenses

OFAC has the authority, through a licensing process, to permit certain transactions that would otherwise be prohibited under its regulations. OFAC can issue a license to engage in an otherwise prohibited transaction when it determines that the transaction does not undermine the U.S. policy objectives of the particular sanctions program, or is otherwise justified by U.S. national security or foreign policy objectives. OFAC can also promulgate general licenses, which authorize categories of transactions, such as allowing reasonable service charges on blocked accounts, without the need for case-by-case authorization from OFAC. These licenses can be found in the regulations for each sanctions program (31 CFR, Chapter V (Regulations)) and may be accessed from the OFAC Web site. Before processing transactions that may be covered under a general license, banks should verify that such transactions meet the relevant criteria of the general license.¹⁵⁴

Specific licenses are issued on a case-by-case basis.¹⁵⁵ A specific license is a written document issued by OFAC authorizing a particular transaction or set of transactions generally limited to a specified time period. To receive a specific license, the person or

¹⁵⁴ License information for a particular sanction program is available on [the OFAC Web site](#) or by contacting OFAC's Licensing area at (202) 622-2480.

¹⁵⁵ Applications for a specific license may be submitted either online from [the OFAC Web site](#), or in writing to: Licensing Division, Office of Foreign Assets Control, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

entity who would like to undertake the transaction must submit an application to OFAC. If the transaction conforms to OFAC's internal licensing policies and U.S. foreign policy objectives, the license generally is issued. If a bank's customer claims to have a specific license, the bank should verify that the transaction conforms to the terms and conditions of the license (including the effective dates of the license), and may wish to obtain and retain a copy of the authorizing license for recordkeeping purposes.

OFAC Reporting

Banks must report all blockings to OFAC within 10 business days of the occurrence and annually by September 30 concerning those assets blocked (as of June 30).¹⁵⁶ Once assets or funds are blocked, they should be placed in a separate blocked account. Prohibited transactions that are rejected must also be reported to OFAC within 10 business days of the occurrence.¹⁵⁷

Banks must keep a full and accurate record of each rejected transaction for at least five years after the date of the transaction. For blocked property (including blocked transactions), records must be maintained for the period the property is blocked and for five years after the date the property is unblocked.

Additional information concerning OFAC regulations, such as Sanctions Program and Country Summaries brochures; the SDN and other lists, including both entities and individuals; recent OFAC actions; and "Frequently Asked Questions," can be found on the OFAC Web site.¹⁵⁸

OFAC Compliance Program

While not required by specific regulation, but as a matter of sound banking practice and in order to mitigate the risk of noncompliance with OFAC requirements, banks should establish and maintain an effective, written OFAC compliance program that is commensurate with their OFAC risk profile (based on products, services, customers, and geographic locations). The program should identify higher-risk areas, provide for appropriate internal controls for screening and reporting, establish independent testing for compliance, designate a bank employee or employees as responsible for OFAC compliance, and create training programs for appropriate personnel in all relevant areas of the bank.

OFAC Risk Assessment

A fundamental element of a sound OFAC compliance program is the bank's assessment of its specific product lines, customer base, and nature of transactions and identification of higher-risk areas for potential OFAC sanctions risk. The initial identification of higher-risk customers for purposes of OFAC may be performed as part of the bank's CIP and CDD procedures. As OFAC sanctions can reach into virtually all areas of its operations, banks should consider all types of transactions, products, and services when conducting their risk

¹⁵⁶ The annual report is to be filed on form TD F 90-22.50.

¹⁵⁷ Reporting, procedures, and penalties regulations, 31 CFR Part 501.

¹⁵⁸ This information is available on [the OFAC Web site](#), or by contacting OFAC's hot line at (202) 622-2490 or toll-free at (800) 540-6322.

assessment and establishing appropriate policies, procedures, and processes. An effective risk assessment should be a composite of multiple factors (as described in more detail below), and depending upon the circumstances, certain factors may be weighed more heavily than others.

Another consideration for the risk assessment is account and transaction parties. New accounts should be compared with OFAC lists prior to being opened or shortly thereafter. However, the extent to which the bank includes account parties other than accountholders (e.g., beneficiaries, guarantors, principals, beneficial owners, nominee shareholders, directors, signatories, and powers of attorney) in the initial OFAC review during the account opening process, and during subsequent database reviews of existing accounts, depends on the bank's risk profile and available technology.

Based on the bank's OFAC risk profile for each area and available technology, the bank should establish policies, procedures, and processes for reviewing transactions and transaction parties (e.g., issuing bank, payee, endorser, or jurisdiction). Currently, OFAC provides guidance on transactions parties on checks. The guidance states if a bank knows or has reason to know that a transaction party on a check is an OFAC target, the bank's processing of the transaction would expose the bank to liability, especially personally handled transactions in a higher-risk area. For example, if a bank knows or has a reason to know that a check transaction involves an OFAC-prohibited party or country, OFAC would expect timely identification and appropriate action.

In evaluating the level of risk, a bank should exercise judgment and take into account all indicators of risk. Although not an exhaustive list, examples of products, services, customers, and geographic locations that may carry a higher level of OFAC risk include:

- International funds transfers.
- Nonresident alien accounts.
- Foreign customer accounts.
- Cross-border ACH transactions.
- Commercial letters of credit and other trade finance products.
- Transactional electronic banking.
- Foreign correspondent bank accounts.
- Payable through accounts.
- Concentration accounts.
- International private banking.
- Overseas branches or subsidiaries.

Appendix M (“Quantity of Risk — OFAC Procedures”) provides guidance to examiners on assessing OFAC risks facing a bank. The risk assessment can be used to assist the examiner

in determining the scope of the OFAC examination. Additional information on compliance risk is posted by OFAC on its Web site under “Frequently Asked Questions.”¹⁵⁹

Once the bank has identified its areas with higher OFAC risk, it should develop appropriate policies, procedures, and processes to address the associated risks. Banks may tailor these policies, procedures, and processes to the specific nature of a business line or product. Furthermore, banks are encouraged to periodically reassess their OFAC risks.

Internal Controls

An effective OFAC compliance program should include internal controls for identifying suspect accounts and transactions, as well as reporting blocked and rejected transactions to OFAC. Internal controls should include the following elements:

Identifying and reviewing suspect transactions. The bank’s policies, procedures, and processes should address how the bank identifies and reviews transactions and accounts for possible OFAC violations, whether conducted manually, through interdiction software, or a combination of both. For screening purposes, the bank should clearly define its criteria for comparing names provided on the OFAC list with the names in the bank’s files or on transactions and for identifying transactions or accounts involving sanctioned countries. The bank’s policies, procedures, and processes should also address how the bank determines whether an initial OFAC hit is a valid match or a false hit.¹⁶⁰ A high volume of false hits may indicate a need to review the bank’s interdiction program.

The screening criteria used by banks to identify name variations and misspellings should be based on the level of OFAC risk associated with the particular product or type of transaction. For example, in a higher-risk area with a high-volume of transactions, the bank’s interdiction software should be able to identify close name derivations for review. The SDN list attempts to provide name derivations; however, the list may not include all derivations. More sophisticated interdiction software may be able to catch variations of an SDN’s name not included on the SDN list. Banks with lower OFAC risk and those with low volumes of transactions may decide to manually filter for OFAC compliance. Decisions to use interdiction software and the degree of sensitivity of that software should be based on a bank’s assessment of its risk and the volume of its transactions. In determining the frequency of OFAC checks and the filtering criteria used (e.g., name derivations), banks should consider the likelihood of incurring a violation and available technology. In addition, banks should periodically reassess their OFAC filtering system. For example, if a bank identifies a name derivation of an OFAC target, then OFAC suggests that the bank add the name to its filtering process.

New accounts should be compared with the OFAC lists prior to being opened or shortly thereafter (e.g., during nightly processing). Banks that perform OFAC checks after account opening should have procedures in place to prevent transactions, other than initial deposits, from occurring until the OFAC check is completed. Prohibited transactions conducted prior

¹⁵⁹ This guidance is available on [the OFAC Web site](#).

¹⁶⁰ Due diligence steps for determining a valid match are provided in *Using OFAC’s Hot line* [on the OFAC Web site](#).

to completing an OFAC check may be subject to possible enforcement action. In addition, banks should have policies, procedures, and processes in place to check existing customers when there are additions or changes to the OFAC list. The frequency of the review should be based on the bank's OFAC risk. For example, banks with a lower OFAC risk level may periodically (e.g., weekly, monthly or quarterly)) compare the customer base against the OFAC list. Transactions such as funds transfers, letters of credit, and noncustomer transactions should be checked against OFAC lists prior to being executed. When developing OFAC policies, procedures, and processes, the bank should keep in mind that OFAC considers the continued operation of an account or the processing of transactions post-designation, along with the adequacy of the bank's OFAC compliance program, to be a factor in determining the appropriate enforcement response to an apparent violation of OFAC regulations.¹⁶¹ The bank should maintain documentation of its OFAC checks on new accounts, the existing customer base and specific transactions.

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 responsibility performed by a third party, the bank is ultimately responsible for that third party's compliance with the OFAC requirements. As a result, banks should have a written agreement in place and establish adequate controls and review procedures for such relationships.

Updating OFAC lists. A bank's OFAC compliance program should include policies, procedures, and processes for timely updating of the lists of sanctioned countries and blocked entities, and individuals, and disseminating such information throughout the bank's domestic operations and its offshore offices, branches and, in the case of Iran and Cuba, foreign subsidiaries. This would include ensuring that any manual updates of interdiction software are completed in a timely manner.

Screening Automated Clearing House (ACH) transactions. ACH transactions may involve persons or parties subject to the sanctions programs administered by OFAC. Refer to the expanded overview section, "Automated Clearing House Transactions," page 216, for additional guidance. OFAC has clarified its interpretation of the application of OFAC's rules for domestic and cross-border ACH transactions and provided more detailed guidance on international ACH transactions.¹⁶²

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

If an ODFI receives domestic ACH transactions that its customer has already batched, the ODFI is not responsible for unbatching those transactions to ensure that no transactions

¹⁶¹ Refer to 74 *Fed. Reg.* 57593 (November 9, 2009), [Economic Sanctions Enforcement Guidelines](#). Further information is available on the [OFAC Web site](#).

¹⁶² Refer to [Guidance to National Automated Clearing House Association \(NACHA\) on cross-border ACH transactions](#).

violate OFAC's regulations. If an ODFI unbatches a file originally received from the Originator in order to process "on-us" transactions, that ODFI is responsible for the OFAC compliance for the on-us transactions because it is acting as both the ODFI and the RDFI for those transactions. ODFIs acting in this capacity should already know their customers for the purposes of OFAC and other regulatory requirements. For the residual unbatched transactions in the file that are not "on-us," as well as those situations where banks deal with unbatched ACH records for reasons other than to strip out the on-us transactions, banks should determine the level of their OFAC risk and develop appropriate policies, procedures, and processes to address the associated risks. Such policies might involve screening each unbatched ACH record. Similarly, banks that have relationships with third-party service providers should assess those relationships and their related ACH transactions to ascertain the bank's level of OFAC risk and to develop appropriate policies, procedures, and processes to mitigate that risk.

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

Due diligence for an inbound or outbound IAT may include screening the parties to a transaction, as well as reviewing the details of the payment field information for an indication of a sanctions violation, investigating the resulting hits, if any, and ultimately blocking or rejecting the transaction, as appropriate. Refer to the expanded overview section, "Automated Clearing House Transactions," page 216, for additional guidance.

Additional information on the types of retail payment systems (ACH payment systems) is available in the FFIEC *Information Technology Examination Handbook*.¹⁶³

In guidance issued on March 10, 2009, OFAC authorized institutions in the United States when they are acting as an ODFI/Gateway Operator (GO) for inbound IAT debits to reject transactions that appear to involve blockable property or property interests.¹⁶⁴ The guidance further states that to the extent that an ODFI/GO screens inbound IAT debits for possible OFAC violations prior to execution and in the course of such screening discovers a potential OFAC violation, the suspect transaction is to be removed from the batch for further investigation. If the ODFI/GO determines that the transaction does appear to violate OFAC regulations, the ODFI/GO should refuse to process the transfer. The procedure applies to transactions that would normally be blocked as well as to transactions that would normally be rejected for OFAC purposes based on the information in the payment.

Reporting. An OFAC compliance program should also include policies, procedures, and processes for handling validly blocked or rejected items under the various sanctions

¹⁶³ Refer to the FFIEC *Information Technology Examination Handbook's* [Retail Payment Systems](#) booklet.

¹⁶⁴ Refer to [the NACHA Web site](#).

programs. When there is a question about the validity of an interdiction, banks can contact OFAC by phone or e-hot line for guidance. Most other items should be reported through usual channels within ten days of the occurrence. The policies, procedures, and processes should also address the management of blocked accounts. Banks are responsible for tracking the amount of blocked funds, the ownership of those funds, and interest paid on those funds. Total amounts blocked, including interest, must be reported to OFAC by September 30 of each year (information as of June 30). When a bank acquires or merges with another bank, both banks should take into consideration the need to review and maintain such records and information.

Banks no longer need to file SARs based solely on blocked narcotics- or terrorism-related transactions, as long as the bank files the required blocking report with OFAC. However, because blocking reports require only limited information, if the bank is in possession of additional information not included on the OFAC blocking report, a separate SAR should be filed with FinCEN that would include such information. In addition, the bank should file a SAR if the transaction itself would be considered suspicious in the absence of a valid OFAC match.¹⁶⁵

Maintaining license information. OFAC recommends that banks consider maintaining copies of customers' OFAC licenses on file. This allows the bank to verify whether a customer is initiating a legal transaction. Banks should also be aware of the expiration date on the OFAC license. If it is unclear whether a particular transaction would be authorized under the terms of the license, the bank should contact OFAC. Maintaining copies of OFAC licenses also is useful when another bank in the payment chain requests verification of a license's validity. Copies of OFAC licenses should be maintained for five years, following the most recent transaction conducted in accordance with the license.

Independent Testing

Every bank should conduct an independent test of its OFAC compliance program that is performed by the internal audit department, outside auditors, consultants, or other qualified independent parties. For large banks, the frequency and area of the independent test should be based on the known or perceived risk of specific business areas. For smaller banks, the audit should be consistent with the bank's OFAC risk profile or be based on a perceived risk. The person(s) responsible for testing should conduct an objective, comprehensive evaluation of OFAC policies, procedures, and processes. The audit scope should be comprehensive enough to assess OFAC compliance risks and evaluate the adequacy of the OFAC compliance program.

Responsible Individual

It is recommended that every bank designate a qualified individual(s) to be responsible for the day-to-day compliance of the OFAC compliance program, including changes or updates to the various sanctions programs, and the reporting of blocked or rejected transactions to OFAC and the oversight of blocked funds. This individual should have an appropriate level of knowledge about OFAC regulations commensurate with the bank's OFAC risk profile.

¹⁶⁵ Refer to FinCEN Release Number 2004-02, [Unitary Filing of Suspicious Activity and Blocking Reports](#), 69 *Fed. Reg.* 76847 (December 23, 2004).

Training

The bank should provide adequate training for all appropriate employees on its OFAC compliance program, procedures and processes. The scope and frequency of the training should be consistent with the bank's OFAC risk profile and appropriate to employee responsibilities.