Practical OFAC Principles for Banks and Financial Institutions

Navigating OFAC demands a map. Access valuable information and key details to stay informed.

February 2010
Introduction
This white paper introduces the Office of Foreign Assets Control (OFAC) and the procedures that institutions should follow to comply with OFAC regulations. This document is NOT intended as legal advice. It is meant to be a plain-English resource that will help clarify OFAC regulations and provide you with the knowledge to develop a sound OFAC compliance program. LexisNexis® has provided a checklist at the end of this white paper to assist you in creating OFAC compliance policies and procedures.

What is OFAC?
The United States Government used economic sanctions as early as the 1800s, but OFAC was formally created in 1950 following a national emergency when China entered into the Korean War. Today, OFAC administers and enforces economic sanctions that the U.S. government determines are necessary based on foreign policy or national security goals. Reasons an entity might be targeted by a sanctions program include participation in activities, such as international narcotics trafficking, human rights violations, terrorism or the proliferation of weapons of mass destruction.

There are approximately 30 different sanctions programs currently under OFAC's management. Many of the sanctions are based on United Nations and other international mandates and involve close cooperation between U.S. government agencies as well as allied governments. Whether multilateral or unilateral, U.S. sanctions programs seek to isolate targets by preventing access to financial assets. This is typically accomplished by controlling financial transactions, import/export activities and travel. OFAC administers and enforces sanctions programs in all of these areas.

Each sanctions program supports different foreign policy and national security goals; thus, prohibited activities (and related compliance requirements) will vary between programs. Although OFAC's programs differ in terms of their scope and application, they all involve the exercise of the President's constitutional and statutory wartime and national emergency powers to impose controls on transactions and trade, and to freeze foreign assets that come within the jurisdiction of the United States\(^1\). The bottom line is that anyone who must comply with OFAC regulations should not violate the laws OFAC administers.

Who must comply
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. incorporated entities and their foreign branches\(^2\)

Some OFAC sanctions also require compliance from:
- Foreign subsidiaries of U.S. companies
- Foreign persons in possession of U.S. origin goods

U.S. persons and entities are expected to exercise due diligence in order to prevent doing business with a sanctioned country, group or individual. In order to detect an entity or person subject to OFAC sanctions, it is prudent to screen all parties to business transactions, including those with direct and indirect involvement. Financial institutions should consult their legal counsel or their federal functional regulators to verify that their compliance program and procedures are suitable for their unique situation. Non-financial institutions should seek advice from their legal representatives.
counsel for compliance program standards. Trade organizations are often good sources of information about how regulations apply to specific industries.

**Who enforces OFAC sanctions programs**

OFAC has the authority to audit businesses on site, but they frequently rely on federal functional regulators to enforce OFAC compliance in markets that are federally regulated. For those markets that are not federally regulated, OFAC itself will audit those businesses. For example, if you are a car dealer, OFAC can audit your business for compliance. In the instances where a business is regulated (such as securities, banks, credit unions, savings and loans, etc.), OFAC relies on the regulator to examine for compliance.

Although more detailed requirements and prohibitions of U.S. sanctions programs are discussed below, OFAC’s basic requirement is that institutions do not violate the laws that it administers. In furtherance of this requirement, OFAC has specific expectations beyond the basic legal prohibitions with regard to the processing of transactions involving certain countries, entities and individuals in order to ensure compliance with U.S. sanctions programs.

Federal and state regulatory agencies review financial institutions under their supervision and enforce OFAC compliance. Regulators ensure compliance through on site examinations in which they review institutions’ policies and procedures, inspect documentation of past and pending transactions and interview personnel.

The primary federal regulators include:

- Federal Deposit Insurance Corporation (FDIC)
- Financial Crimes Enforcement Network (FinCEN)
- Board of Directors of the Federal Reserve System (FED)
- National Credit Union Administration (NCUA)
- Office of the Comptroller of the Currency (OCC)
- Office of Thrift Supervision (OTS)
- Securities Exchange Commission (SEC)

OFAC enforces compliance within non-financial industries through the combined efforts and oversight of various government agencies and the federal law enforcement community, depending on the organization, the applicable sanction and the nature of the violation.

**U.S. sanction legislation**

OFAC administers approximately 30 different sanctions programs. You should devote time to review the laws, rules and regulations that provide the legal framework for each of the sanctions programs. A few of the significant pieces of legislation connected with OFAC embargoed countries and criminal penalties are:

- Trading with the Enemy Act
- International Emergency Economic Powers Act
- United Nations Participation Act
- International Security and Development Cooperation Act
- The Cuban Liberty and Democratic Solidarity
- The Antiterrorism and Effective Death Penalty Act
- The Foreign Narcotics Kingpin Designation Act
OFAC administers two broad categories of economic sanctions and embargoes: those that target geographic regions and governments and those targeting individuals or entities that could be anywhere. OFAC publishes an index of sanctions programs and countries summaries on its website. It also publishes a list of the names of companies and individuals designated under programs that are not country-specific. These targets are located throughout the world; in fact, a number of them are known to move from country to country.

The list of specific entities and persons that are designated under the various sanctions programs comprises OFAC’s list of Specially Designated Nationals and Blocked Persons—the SDN list, which includes individuals, groups and entities involved in criminal activity such as terrorism, narcotics trafficking, human rights violations, the proliferation of weapons of mass destruction or interfering with international stabilization efforts. OFAC publishes the list of SDNs at its website.

The index of OFAC Country sanctions programs contains links to overview information for each sanctions program, as well as interpretive guidance, general licenses issued and additional information on the laws, rules and regulations that provide the legal framework for the program. You need to devote time and attention to understand the anatomy of an OFAC Sanction Program, so that you know how to read through and understand them on a regular basis. They change on an unpredictable schedule.

The type of sanctions applied to a particular country, organization, group or individual may vary across sanctions programs. Exact regulations vary because each sanctions program is rooted in specific goals in foreign policy or national security. Sanctions programs may contain an annex which specifies individuals or entities against which sanctions are intended. Often, but not always, the names of such entities are also included on the SDN list.

Overall, OFAC sanctions typically prohibit or at least restrict U.S. persons and entities from doing business with designated individuals, groups, companies or countries. Activities that may be restricted include imports, exports (including exports of financial services), travel or financial transactions.

Financial sanctions are achieved through two primary mechanisms: “rejecting” a transaction and “blocking” foreign assets under U.S. jurisdiction.

<table>
<thead>
<tr>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Blocking</strong> a transaction involves accepting the funds intended for the transaction and then freezing those funds or accounts so that the owner is effectively denied access. Blocking can occur when a customer initiates a transaction at an institution or moves funds through an institution during a transfer. Assets remain blocked until OFAC grants permission for access.</td>
</tr>
<tr>
<td><strong>Rejecting</strong> a transaction entails refusing to conduct or participate in the transaction. Rejecting can occur when a transaction is initiated at an institution or when funds are moving through an institution in a transfer.</td>
</tr>
</tbody>
</table>

Generally speaking, if an entity is included on OFAC’s SDN list, the assets must be blocked. OFAC also publishes a list of entities association with the Palestinian Legislative Council whose transactions you should not block, but, rather,
reject. Depending on the particular transaction and program, either blocking or rejecting may be required. Again, these vary because they are rooted in specific foreign policy or national security goals.

**Transactions subject to OFAC sanctions programs**
Institutions should conduct a risk analysis to determine the likelihood that they will encounter OFAC issues. Certain types of business operations, such as international wire transfers or international trade (particularly trade finance) are at a higher risk than others. Your OFAC-related risk depends in large part on who your customers are and what kind of business you do. Your OFAC compliance program should be commensurate with and address the particular areas of risk associated with your business operations. LexisNexis, regulators and OFAC all agree that businesses should take a risk-based approach to compliance.

The consequences of compliance failure can be substantial. What if it is discovered that your company transferred funds to a terrorist or drug trafficker? Likely, your company will be subject to an enforcement action and suffer negative publicity. The impact of reputational damage can be devastating; it can cripple or even destroy an organization.

It is therefore prudent to incorporate OFAC compliance steps into procedures for completing most transactions. In order to detect problems before they occur, these compliance steps should be enacted before a transaction is complete. For example, new accounts should be checked at account opening.

Transactions that may necessitate OFAC sanctions compliance steps include, but are not limited to, the following:  
• Deposit accounts (checking, savings, money market accounts, etc.)  
• Loans  
• Lines of credit  
• Letters of credit  
• Safety deposit boxes  
• Wire transfers  
• ACH (Automated Clearing House) transfers  
• Currency exchanges  
• Depositing or cashing checks  
• Purchase of money orders, cashier’s checks or traveler’s checks  
• Loan payments  
• Guarantors and collateral owners  
• Trust accounts  
• Credit cards

Compliance tip
Institutions should identify a compliance officer responsible for understanding and educating staff about the unique requirements of each OFAC sanctions program and the specific foreign policy that it supports.
Ideally, institutions should check the names of all parties involved in every transaction against OFAC lists (SDN, Non-SDN and OFAC Sanctions Program list).

**OFAC licensing**

OFAC grants licenses allowing transactions to occur that would otherwise be prohibited by regulations. For example, under certain sanctions programs, humanitarian aid may be allowed in countries where other import/export activity is not allowed, as long as the requirements of the license are met. There are two types of OFAC licenses: specific and general.

**General** licenses are actually exceptions to the general prohibitions that are contained in the regulations pertaining to a particular sanctions program. Unlike specific licenses, general licenses do not require institutions to request permission from OFAC before engaging in a transaction covered by the license. Rather, general licenses allow transactions by entities who meet all established criteria and required conditions identified in the regulations without seeking authorization. As this suggests, it is critical that institutions are certain that a general license applies before proceeding with a transaction based on such a license.

**Specific** licenses are sometimes granted by OFAC in response to an application for a specific type of transaction, by a specific entity, at a specific time. License requests for proposed transactions or activities do not have to be submitted on a particular form. However, applicants may use the Application for the Release of Blocked Funds form. Each application should contain the following information:

- Detailed description of the proposed transaction
- Names and addresses for any individuals/companies involved
- Any specific information required by the sanction

**Compliance tip**

When checking transactions for OFAC compliance, remember to check beneficiaries, collateral owners, guarantors, cosigners, receiving parties, sending parties and any other party to the transaction, as applicable.
Release of blocked funds
If the owner of a blocked account wants to apply to OFAC for the release of funds, the owner should use the Application for the Release of Blocked Funds form found at the OFAC website. This form is required for requests and should include all relevant information, including a comprehensive explanation of any underlying transactions and the names and addresses of all of the parties involved. LexisNexis recommends attaching a photocopy of all associated transaction documents. Three copies of application materials should be mailed (not faxed) to OFAC at:
Office of Foreign Assets Control
U.S. Department of the Treasury
Treasury Annex
1500 Pennsylvania Avenue, NW
Washington, DC 20220
Attn: Licensing Division

OFAC violations
An institution’s failure to comply with the laws that OFAC administers can jeopardize critical foreign policy and national security goals. In light of this, OFAC can levy heavy penalties for non-compliance. Civil penalties range from $11,000 to $1 million, and criminal penalties can include fines ranging from $50,000 to $10 million plus imprisonment for willful violations. OFAC may take the following factors into consideration when determining whether to levy civil or criminal penalties for a violation:
• The extent of the institution’s compliance efforts
• The comprehensiveness of the OFAC compliance policies and procedures, and how appropriate it is to the organization’s risk
• How the institution monitors transactions for compliance with OFAC regulations (e.g., whether it uses interdiction software, etc.)

OFAC does not grant amnesty for voluntary disclosure of past violations, but self-disclosure may be considered a mitigating factor when OFAC reviews the circumstances surrounding any violation. If an institution becomes aware that it may have violated OFAC regulations, LexisNexis recommends it contact its legal counsel immediately. Voluntary disclosure of such violations shows good corporate citizenship, and if institutions decide to voluntarily disclose a violation, they should do so by writing a letter to OFAC.
In January of 2006, OFAC published new enforcement procedures for banking institutions. These enforcement procedures provide a general framework for OFAC enforcement actions, but these procedures only address banking institutions. OFAC has indicated that it will issue similar procedures for other industries. The new enforcement procedures take into account that each institution’s situation is different and that its compliance program should be tailored to its unique circumstances. This includes an analysis of its size, business volume, customer base and product lines.

### Compliance procedures

To ensure compliance, an institution should have a clear and thorough policy and procedure manual, educate and train their employees accordingly and possess an efficient in-depth compliance system that ensures the proper handling of all transactions and customers. Key staff members, including those involved in opening new accounts or handling transactions, should be given sufficient training and information to enable them to recognize and stop suspicious transactions. Documentation of compliance activities by the personnel who conduct the activity will provide evidence of an institution’s efforts to comply.

Refresher training should be provided on a regular basis. Institutions should evaluate the effectiveness of the training to ensure employees know what is expected of them and are following established procedures. In order to determine whether your training program is effective, you should test trainees for content knowledge and audit the activities of personnel. Knowing what to do and choosing to take action, on the part of the employee, are two different things. An examination at the conclusion of a training session will test for comprehension of compliance regulations, but an audit will show whether the knowledge transferred to the workplace. If the audit indicates inadequacies in any particular area, make relevant training a top priority. As with all compliance activities, it is critical that compliance professionals document all training activities and make copies of training materials so that they are available for review by examiners.

Auditing the OFAC compliance program’s policies, procedures and training should be conducted on a regularly scheduled basis. You do not have to hire a consultant to perform such an audit. Companies may use a qualified internal employee to audit or contract with an external auditor. If internal personnel are the auditors, they should have solid OFAC expertise but should not be involved in the compliance function being tested. A report containing the audit findings should be presented directly to the board of directors and senior management, who will subsequently determine the appropriate course of action.

### Compliance tip

While fines for OFAC violations can be substantial, loss of business due to damaged reputation may far outweigh the impact of any fine. In addition, the amount of time demanded of senior management may result in lost opportunities had they been able to focus on strategic planning to benefit the business.

**Compliance tip**

The most important part of a compliance program is knowledge. We recommend that each institution designate an OFAC compliance officer who develops expertise in OFAC sanctions and compliance. There is simply no substitute for a clear understanding of OFAC related issues.
While the frequency of an OFAC audit is not specifically defined in any statute, a sound practice is for [institutions] to conduct independent testing generally every 12 to 18 months. 

**Monitor OFAC**  
Institutions should regularly monitor the OFAC website for new announcements and changes to the listings. Close monitoring will allow the institution to check their client information data against the OFAC information in a timely manner. Close monitoring will also enable institutions to make any appropriate changes to their compliance program in a timely manner.

There is no set schedule for updates to OFAC watchlists as sanctions are based on foreign policy and can be unpredictable as a result. OFAC provides free notification services (email or RSS feeds) to alert subscribers to changes in the SDN list or country-specific sanctions programs.

**Scan customer files**  
OFAC does not legally prescribe the frequency of customer file scans against OFAC-provided lists. The frequency at which an institution scans customer files against OFAC watchlists should be determined by internal policy with guidance from the institution’s regulator, and should reflect the institution's risk factors. To put it simply, OFAC does not tell you how to comply, only that you must comply. LexisNexis offers the following general recommendations for institutions:

- Check each new customer against the current OFAC watchlists.
- Check persons or entities who are involved in transactions against current OFAC watchlists.
- Scan complete customer database initially against OFAC watchlists and whenever OFAC updates its watchlists.
- Scan complete customer database on a regular basis depending upon the institution’s degree of risk.

**Due diligence for potential match**  
It is possible to check your customer files against watchlists manually, but with thousands (or millions) of customers, this is impractical. Also, given that the watchlist contains thousands of entity names and organizations, a manual effort would be costly. Many organizations use software to help them compare their customers’ names to the watchlists. After all, it is a highly clerical task, ideally suited to automation. Software helps speed the comparison times, but it might also generate a large number of alerts regarding possible matches. The software’s job is to alert you of possible matches, but it does not decide whether a possible match is a true match or a false positive. That decision is ultimately made by someone at your organization.

If there is a potential match or hit to an entity on the OFAC list, the institution should perform due diligence to determine if the potential match is an actual match or a false positive. Institutions should:

- Determine whether the hit was generated by the OFAC watchlist. (Some software used for OFAC compliance provides additional watchlists against which to scan).
- If it is a true OFAC match, compare the complete name for similarities and determine if the entity types match (individual, organization or vessel).
- If the entity type matches, and the name is quite similar, then evaluate the overall quality of the hit by comparing the complete OFAC entry with all of the information you have on file for the person in your transaction.
- Request more information than originally obtained from the customer if necessary.
- Compare addresses, date of birth, nationality, tax ID, passport number, driver’s license numbers, place of birth, etc.
• If after further examination, the hit appears to be an actual match, call OFAC at: 800.540.6322 or use OFAC’s e-Hotline system at: www.treas.gov/offices/enforcement/ofac/hotline.shtml.

• Document all steps taken, including calls, notes, etc., in a log that evidences actions taken and decisions made.

Note: A detailed list of OFAC’s recommended due diligence steps can be found at the OFAC website.

The overall goal of any due diligence effort is to ensure that the business you are about to conduct is lawful. Customer identification is an essential component of a sound due diligence program, but your due diligence will not always end by confirming the identity and watchlist match information. Due diligence efforts may also be necessary to determine the nature of the transaction.

By way of example, consider the situation when a potential match is reported against one of OFAC’s country sanctions programs. In order to determine what action is required, if any, all documents related to the particular sanctions program must be evaluated. It is possible that you will need to determine the source of the funds in the transaction to verify that they are not proceeds from drug trafficking, arms sales, terrorist activity, etc. In fact, due diligence may reveal that you will need to monitor all account activity and analyze each and every transaction that involves the customer.

True match
If after due diligence the entity is determined to be a true match, the institution should review the related OFAC sanction to determine appropriate action.

Note: You should take appropriate due diligence steps to make certain that a match is valid. Even if you obtain a match that appears to be a close match (for example, because of a high score), additional research is needed to decide whether you have a true match or false positive. In some cases, the name you enter will be similar to a target’s name, but the rest of the information provided differs from that of the true entity on the watchlist.

Blocking is the most common action taken because U.S. persons are generally prohibited from dealing with entities on the SDN list. However, some matches will require rejecting, and others may be approved depending upon the findings from due diligence efforts. If the sanctions program requires either blocking or rejecting, a report must be filed with OFAC within 10 business days.
Note: The only way to determine the correct action is to thoroughly review the related sanctions program. Remember that each sanctions program is unique.

You can inform the customer that a transaction was rejected or that assets have been blocked. An institution’s policies and procedures should clearly instruct key employees how to handle each situation, including instructions for how and when they should provide such notice to the customer.

The customer has the right to apply for the funds to be released or to obtain a license for the transaction. See “Transactions Subject To OFAC Sanctions Programs” on page 7 for more information.

Note: Not all OFAC matches, if deemed true matches, will involve blocking. Be clear about all potential actions required and when to apply them.

**OFAC reports and record retention**
OFAC requires the retention of all reports and blocked or rejected transaction records for five years.

**Blocked or rejected transactions reports**
Any transaction that has been blocked or rejected must be reported to OFAC within 10 business days from the date the action was taken. The forms required to report these actions are:
- Voluntary Form for Reporting Blocked Transactions
- Voluntary Form for Reporting Rejected Transactions

Note: OFAC makes all of the reports described available on its website.

**Annual Report**
Institutions that have blocked transactions must also report the transactions to OFAC annually. The Annual Report of Blocked Property is due by September 30th of each year. The report details all of the blocked property as of June 30th of the year. OFAC uses this information for planning purposes and to verify compliance. There is no annual reporting of rejected transactions.

Compliance tip
Interdiction software should provide a mechanism for documenting compliance activities. The software may allow for electronic storage of list comparison activity that can be recalled and printed when requested.

Compliance tip
In cases of a true match, the appropriate company officer, usually the compliance officer, should be notified immediately.
OFAC compliance checklist

Use the following checklist as a guide to determine if your institution has the necessary components for a solid OFAC compliance program in place. This checklist is merely exemplary. It is not exhaustive and each institution must develop its own risk analysis and design its own compliance program based on its business operations.

OFAC checklist

• Conduct OFAC risk analysis.
• Identify and designate a person responsible for OFAC compliance in your organization.
• Define and document the purpose of the program and the dedicated resources.
• Develop and document policies and procedures to meet OFAC compliance.
• Obtain management endorsement of your program, policies and procedures.
• Develop and implement OFAC training both for new employees and refresher training.
• Scan customer lists against the OFAC SDN and Sanctions Program lists.
  – Scan ALL new customers (include beneficiaries).
  – Scan ALL customer files after an OFAC list update.
  – Scan ALL customer files on a regular basis.
• If a potential match is identified, perform due diligence.
  – Notify appropriate people in organization.
  – Refer to applicable organization policies and procedures.
• If the potential match is a true match:
  – Review sanction.
  – Notify appropriate people in organization.
  – Refer to applicable organization policies and procedures.
  – Document all procedures and decisions.
  – Report blocked or rejected transaction within 10 business days.
• Report blocked accounts annually.
• Conduct OFAC audits to ensure policies correctly followed.

Compliance tip

An audit trail for each customer should be created and retained that includes names checked, decisions and reasons behind decisions and the status of the customer. Storing this information electronically is an easy way to keep this information. Many software solutions offer this functionality.
Practical OFAC Principles 
for Banks and Financial Institutions

Sources


7. Ibid.


For more information:
Call 866.858.7246 or visit lexisnexis.com/risk/financial-services

About LexisNexis® Risk Solutions
LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

Our financial services solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.

The Bridger Insight XG services are not provided by “consumer reporting agencies,” as that term is defined in the Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.) (“FCRA”) and do not constitute “consumer reports,” as that term is defined in the FCRA. Accordingly, the Bridger Insight XG service may not be used in whole or in part as a factor in determining eligibility for credit, insurance, employment or another purpose in connection with which a consumer report may be used under the FCRA. Due to the nature of the origin of public record information, the public records and commercially available data sources used in reports may contain errors. Source data is sometimes reported or entered inaccurately, processed poorly or incorrectly, and is generally not free from defect. This product or service aggregates and reports data, as provided by the public records and commercially available data sources, and is not the source of the data, nor is it a comprehensive compilation of the data. Before relying on any data, it should be independently verified. LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. Bridger Insight is a trademark of LexisNexis Risk Solutions Inc. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright © 2011 LexisNexis. All rights reserved. NXR01289-2 1211