Appendix 308B

Excerpts from the Federal Financial Institutions Examination Council's BSA/AML Examination Guide on OFAC Compliance

Office of Foreign Asset Control (OFAC)

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

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

All U.S. persons, including U.S. banks, bank holding companies, non-bank subsidiaries and credit unions, must comply with OFAC's regulations. The federal banking agencies evaluate OFAC compliance systems to ensure all financial institutions subject to their supervision comply with the sanctions. 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. In general, the regulations require 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 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. financial institution to an offshore bank, and there is an OFAC-designated party on the transaction, it must be blocked. The definition of assets and property is broad and is defined within

each sanction program. Assets and property includes anything of direct, indirect, present, future, or contingent value (including all types of banking transactions). Financial institutions 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. financial institution 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. A payment order cannot be canceled or amended after it is received by a U.S. financial institution in the absence of an authorization from OFAC.

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. financial institution would have to reject a funds transfer between two companies, which are not Specially Designated Nationals or Blocked Persons (SDNs), involving an export to a company in Sudan that also is not an SDN. Because Sudanese Sanctions would only require blocking transactions with the Government of Sudan or SDNs, there would be no blockable interest in the funds between the two companies. However, because the transactions would constitute support of Sudanese commercial activity, which is prohibited, the U.S. institution cannot process the transaction and would simply reject the transaction.

It is important to note OFAC specifying prohibitions against certain countries, entities, and individuals is separate and distinct from the provision within the BSA's Customer Identification Program (CIP) regulation that requires financial institutions 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. 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 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 OFAC's web site. Before processing transactions that may be covered under a general license, financial institutions should verify such transactions meet the relevant criteria of the general license.

Specific licenses are issued on a case-by-case basis. A specific license is a written document issued by OFAC authorizing a particular transaction or set of transactions. To receive a specific license, the person or entity who would like to undertake the transaction must submit an application to OFAC. If the transaction conforms with U.S. foreign policy under a particular program, the license will be issued. If a financial institution's customer or member claims to have a specific license, the institution should verify the transaction conforms to the terms of the license and obtain and retain a copy of the authorizing license.

OFAC Reporting

Financial institutions must report all blockings to OFAC within ten days of the occurrence and annually by September 30 concerning those assets blocked (as of June 30). Once assets or funds are blocked, they should be placed in a blocked account. Rejected, prohibited transactions must also be reported to OFAC within ten days of the occurrence.

Financial institutions 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 list, including both entities and individuals; recent OFAC actions; and "Frequently Asked Questions," can be found on OFAC's web site.

OFAC Program

While not required by specific regulation, but as a matter of sound "banking" practice and in order to ensure compliance, credit unions should establish and maintain an effective, written OFAC program commensurate with their OFAC risk profile (based on products, services, customers, and geographic locations). The program should identify high-risk areas, provide for appropriate internal controls for screening and reporting, establish independent testing for compliance, designate an employee or employees as responsible for OFAC compliance, and create training programs for appropriate personnel in all relevant areas of the institution. A credit union's OFAC program should be commensurate with its respective OFAC risk profile.

OFAC Risk Assessment

A fundamental element of a sound OFAC program is the credit union's assessment of its specific product lines, customer base, and nature of transactions and identification of the high-risk areas for OFAC transactions. The initial identification of high-risk members for purposes of OFAC may be performed as part of the credit union's CIP and customer due diligence (CDD) procedures. As OFAC sanctions can reach into virtually all areas of its operations, credit unions should consider all types of transactions, products, and services when conducting their risk assessment and establishing appropriate policies, procedures, and processes. An effective risk assessment should be a composite of multiple factors, 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 credit union 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, will depend on the credit union's risk profile and available technology.

Based on the credit union's OFAC risk profile for each area and available technology, the credit union 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 financial institution knows or has reason to know a transaction party on a check is an OFAC target, the processing of the transaction would expose the financial institution to liability, especially personally handled transactions in a high-risk area. For example, if a financial institution knows or has a reason to know 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 credit union should exercise judgment and take into account all indicators of risk. Although not an exhaustive list, examples of products, services, members, and geographic locations that may carry a higher level of OFAC risk include:

- International funds transfers;
- Nonresident alien accounts;
- Foreign member accounts;
- Cross-border automated clearing house (ACH) transactions;
- Commercial letters of credit;
- Transactional electronic banking;
- Foreign correspondent bank accounts;
- Payable through accounts;
- International private banking; and
- Overseas branches or subsidiaries.

In the absence of a credit union performed risk assessment, Appendix M ("Quantity of Risk — OFAC Procedures") in the FFIEC BSA/AML Examination Manual can be used to provide guidance to examiners on assessing OFAC risks facing a credit union. The risk assessment can be used to assist in determining the scope of the OFAC examination. A comprehensive risk assessment is likely to indicate the credit union has sufficient programs and controls in place, allowing the examiner to focus on higher risk areas versus a full program evaluation.

Once a credit union has identified its areas with high OFAC risk, it should develop appropriate policies, procedures, and processes to address the associated risks. Credit unions may tailor these policies, procedures, and processes to the specific nature of a business line or product. Furthermore, it is a sound business practice for a credit union to periodically reassess their OFAC risks. Especially if the credit union offers new products, services, or business lines, or is entering new geographic markets.

Internal Controls

An effective OFAC program should include internal controls for identifying suspect accounts and transactions and reporting to OFAC. Internal controls should include the following elements:

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

The screening criteria used by credit unions 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 high-risk area with a high volume of transactions, the credit union'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. Low-risk credit unions or areas 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 credit union's assessment of its risk and the volume of its transactions. The volume of transactions processed through corporate credit unions generally prohibits manually screening for OFAC matches; automated interdiction software is strongly recommended.

In determining the frequency of OFAC checks and the filtering criteria used (e.g., name derivations), credit unions should consider the likelihood of incurring a violation and available technology. In addition, credit unions should periodically reassess their OFAC filtering system. For example, if a credit union identifies a name derivation of an OFAC target, then OFAC suggests the credit union 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). Credit unions 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 to completing an OFAC check may be subject to possible penalty action.

In addition, credit unions should have policies, procedures, and processes in place to check existing members when there are additions or changes to the OFAC list. The frequency of the review should be based on the credit union's OFAC risk. For example, credit unions with a low OFAC risk level may periodically (e.g., monthly or quarterly) compare the member base against the OFAC list. Transactions such as funds transfers, letters of credit, and non-member transactions should be checked against OFAC lists prior to being executed. When developing OFAC policies, procedures, and processes, the credit union should keep in mind OFAC considers the continued operation of an account or the processing of transactions post-designation, along with the adequacy of their OFAC compliance program, to be a factor in determining penalty actions. The credit union should maintain documentation of its OFAC checks on new accounts, existing members, and specific transactions.

If a credit union 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 credit union is ultimately responsible for that third party's compliance with the OFAC requirements. As a result, credit unions should establish adequate controls and review procedures for such relationships.

Updating OFAC lists. A credit union's OFAC program should include policies, procedures, and processes for timely updating of the lists of blocked countries, entities, and individuals and disseminating such information throughout the credit union's operations and branches. This would include ensuring that any manual updates of interdiction software are completed in a timely manner.

Screening ACH transactions. All parties to an ACH transaction are subject to the requirements of OFAC. OFAC has clarified the application of its rules for domestic and cross-border ACH transactions and is working with industry to provide more detailed guidance on cross-border ACH.

With respect to domestic ACH transactions, the Originating Depository Financial Institution (ODFI) is responsible for verifying the originator is not a blocked party and making a good faith effort to determine the originator is not transmitting blocked funds. The Receiving Depository Financial Institution (RDFI) similarly is responsible for verifying the receiver is not a blocked party. In this way, the ODFI and the RDFI are relying on each other for compliance with OFAC policies. ODFIs are not responsible for unbatching transactions and ensuring they do not process transactions in violation of OFAC's regulations if they receive those transactions already batched from their customers. If the ODFI unbatches the transactions it received from its customers, then the ODFI is responsible for screening as though it had done the initial batching.

With respect to OFAC screening, these same obligations hold for cross-border ACH transactions. For outbound cross-border ACH transactions, however, the ODFI cannot rely on OFAC screening by the RDFI outside of the United States. In the case of inbound ACH transactions, the RDFI is responsible for compliance with OFAC requirements.

Additional information on all types of retail payment systems is available in the FFIEC *Information Technology Examination Handbook*.

Reporting. An OFAC program should also include policies, procedures, and processes for handling items that are valid blocked or rejected items under the various sanctions programs. In the case of interdictions related to narcotics trafficking or terrorism, credit unions should notify OFAC as soon as possible by phone or e-hotline about potential hits with a follow-up in writing within ten days. 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. Credit unions 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 credit union acquires or merges with another credit union, both credit unions should take into consideration the need to review and maintain such records and information.

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

Maintaining license information. OFAC recommends credit unions consider maintaining copies of members' OFAC licenses on file. This will allow the credit union to verify whether a member is initiating a legal transaction. Credit unions should also be aware of the expiration date on the license. If it is unclear whether a particular transaction is authorized by a license, the credit union should confirm with OFAC. Maintaining copies of licenses will also be useful if another financial institution in the payment chain requests verification of a license's validity. Copies of licenses should be maintained for five years, following the most recent transaction conducted in accordance with the license.

Independent Testing

Every credit union should conduct an independent test of its OFAC program that is performed by the internal audit department, outside auditors, consultants, or other qualified independent parties. For large credit unions, the frequency and area of the independent test should be based on the known or perceived risk of specific business areas. For smaller credit unions, the audit should be consistent with the credit union'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 program.

Responsible Individual

It is recommended every credit union designate a qualified individual(s) to be responsible for the day-to-day compliance of the OFAC program, including 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 credit union's OFAC risk profile.

Training

The credit union should provide adequate training for all applicable employees. The scope and frequency of the training should be consistent with the credit union's OFAC risk profile and appropriate to employee responsibilities.