# OFAC COMPLIANCE POLICY

Meyer Sound Laboratories, Incorporated.

# Table of Contents

## Introduction

The U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") administers and oversees a series of laws, regulations, and executive orders that impose economic sanctions against hostile targets to further U.S. foreign policy and national security objectives. OFAC has a broad mandate to administer, promulgate, and enforce these various sanction regimes.

OFAC's sanctions enforcement function benefits from coordination with various federal law enforcement agencies covering the entire spectrum of international trade (e.g., FBI, Customs and Border Protection, Homeland Security Investigations, Bureau of Industry and Security, etc.). All of these agencies help OFAC enforce the sanctions. OFAC also has the power to subpoena U.S. persons and businesses in the course of its investigations. Additionally, most of the reputable financial institutions around the globe internally enforce U.S. economic sanctions through their respective compliance offices.

Depending on the legal requirements of the particular sanctions program implicated, financial institutions will reject or freeze their customers' transactions and report their customers' possible violations to OFAC. Sensitivity to sanctions liability is recognized throughout the globe and recent enforcement actions have resulted in multi-million dollar fines and terms of imprisonment for perpetrators. Sanctions compliance must therefore be a priority at Meyer Sound.

Moreover, the objective of economic sanctions is to diminish the capabilities of hostile targets by denying them access to the U.S. economic system. Accordingly, to accomplish this, sanctions broadly prohibit all U.S. persons and U.S. businesses from engaging in transactions, directly or indirectly, with those targets. Those targets can be entire nations, business networks, entities, and individuals. And the only way sanctions against hostile targets can be effective at shaping foreign policy is when U.S. persons and U.S. businesses comply with the prohibitions proscribed in them. It has been and continues to be Meyer Sound's policy to comply with all OFAC sanctions. In furtherance of this policy and to protect the company and its employees from liability and to further U.S. foreign policy and national security objectives, Meyer Sound seeks to better educate its employees regarding OFAC sanctions and has adopted comprehensive written OFAC compliance policy and compliance protocols. This document serves as a statement of Meyer Sound's OFAC compliance policy.

The purpose of this document is to provide (1) an overview of OFAC and economic sanctions generally; (2) an outline of best practices in OFAC compliance; (3) general information on how to screen transactions for potential violations; (4) information on how to proceed after a possible violation is discovered; and (5) an outline

of the OFAC-related document retention policy. To assist in the implementation of this policy, Meyer Sound will provide its employees with separate abbreviated OFAC compliance guidelines and protocols to follow in connection with the sale of its products and services.

## Meyer Sound's OFAC Risk Profile

Meyer Sound has a relatively high OFAC risk profile because it conducts business in all regions of the world. Moreover, under U.S. law, a U.S. parent company is liable for the OFAC violations of its controlled or owned foreign subsidiaries and also can be liable for violations by its independent contractors. And because the prohibitions of the sanctions are broadly construed and have no intent requirement (strict liability for violations), Meyer Sound must minimize risk by appropriately screening its transactions, including where appropriate scrutinizing the parties in the transactional chain, and red flagging potential violations for closer review by senior management or outside counsel.

Meyer Sound, through all of its employees and contractors, must remain vigilant and execute appropriate transactional due diligence before finalizing, executing, and performing any sales agreement. Any employee that can speak for, bind, or otherwise obligate the company to a transaction or agreement must be alert to and flag potential violations of OFAC sanctions as described in this manual and shall follow OFAC compliance protocols established by the company.

Although all employees should be able to identify possible violations and know to report such violations to senior management, the responsibility of OFAC compliance will fall primarily upon Sales, Finance, Technical Support, Design Services, and Service departments. Those departments have the most exposure to foreigners and global trade, and therefore, are most exposed to OFAC liability.

*Audits of Compliance Program*

To ensure Meyer Sound's own internal compliance with this policy, periodic audits may be performed to ensure transactions are being properly scrutinized. Such audits may be performed by senior management in the Sales, Finance, Technical Support, Design Services, or Service departments. Employees will not be informed of when an audit will take place.

## Meyer Sound's OFAC Compliance Leadership

The Vice President of Worldwide Sales and the Chief Financial Officer will provide OFAC guidance and leadership to all members of their respective departments and shall be primarily responsible for implementing OFAC compliance protocols established by the company. Members of the sales team should report any possible OFAC violations to the VP of Worldwide Sales and members of the finance team, including personnel responsible for sales order entry, should report any possible OFAC violations to the CFO.

The Directors of Technical Support, Director of Service Worldwide, Design Services Manager, and the Customer Service/Sales Supervisor should also be apprised of all OFAC-related matters and trainings, as their departments may also be exposed to possible violations. These two departments are also uniquely situated to determine whether possible violation went unnoticed in the past. For example, if an end-user who resides in a sanctioned country calls or emails for support, the employee reviewing the inquiry should immediately notify their Director and an internal investigation should ensue.

If for any reason an employee feels it necessary to bypass the VP of Worldwide Sales, the CFO, or the Directors of Technical Support, Director of Service Worldwide, Design Services Manager, and the Customer Service/Sales Supervisor with respect to an OFAC related matter, that employee should address their concerns to the Executive Vice President or her designee.

All employees, regardless of the department they work in, may report possible OFAC violations to the Executive Vice President or her designee. Senior management should also direct all OFAC related concerns or questions to the Executive Vice President.

When appropriate, legal counsel will be engaged to evaluate a transaction or possible violation.

## OFAC Sanctions

OFAC administers and enforces economic sanctions programs primarily against countries and groups of individuals, such as terrorists and narcotics traffickers. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals.

Sanctions are, in essence, laws that impose a broad range of transactional prohibitions. Prohibited transactions can consist of nearly all commercial or financial transactions with targeted countries. Prohibited transactions can also include nearly all commercial or financial transactions with particular persons, individuals, and entities identified by OFAC. Furthermore, the sanctions can prohibit other dealings in which U.S. persons may not engage unless authorized by OFAC or expressly exempted by statute. Because each sanctions program is based on different foreign policy and national security goals, specific prohibitions may vary between programs.

Federal statutes and presidential executive orders serve as the basis for OFAC-administered sanctions programs. The three most prominent federal statutes that empower the president to designate targets of economic sanctions are the International Emergency Economic Powers Act, the Trading with the Enemy Act and the Antiterrorism and Effective Death Penalty Act. Under these statutes and related executive orders, sanctions programs may be either unilateral (administered only by the US) or multilateral (administered in coordination with other countries).

It is important to note that in non-comprehensive programs, there are no broad prohibitions on dealings with countries, but only against specific named individuals and entities. The names are incorporated into OFAC's list of Specially Designated Nationals and Blocked Persons ("SDN List") which includes over 6,000 names of companies and individuals who are connected with the sanctions targets. A number of the named individuals and entities are known to move from country to country and may end up in locations where they would be least expected. U.S. persons are prohibited from dealing with SDNs wherever they are located and all SDN assets are blocked. Entities that a person on the SDN List owns (defined as a direct or indirect ownership interest of 50% or more) are also blocked, regardless of whether that entity is separately named on the SDN List. Because OFAC's programs are dynamic and constantly changing, it is important to check OFAC's website on a regular basis to ensure the SDN List is current and you have complete information regarding current restrictions affecting countries and parties with which you plan to do business.

Compliance is important for two primary reasons. First, sanctions are an extension of U.S. foreign policy and national security objectives. Complying with the

sanctions furthers the stated goals of the U.S. government. Non-compliance tends to harm or undermine U.S. national security and foreign policy goals. This is why OFAC related violations often carry stiff penalties and lengthy terms of imprisonment, which is the second reason compliance is important.

*Fines and/or Imprisonment*

The fines for violations can be substantial. Depending on the program, criminal penalties can include fines ranging from $50,000 to $10,000,000 and imprisonment ranging from 10 to 30 years for willful violations. Depending on the sanctions program and the seriousness of the violation, civil penalties can range up to a per violation statutory maximum of $250,000 or twice the amount of each underlying transaction, whichever is higher.

*Terminology*

The term "*U.S. persons*" includes any U.S. citizen or U.S. permanent resident anywhere in the world, any U.S. business entity and its foreign subsidiaries anywhere in the world, and all persons and businesses physically present in the United States. As was stated before, all U.S. persons must comply with OFAC regulations. Meyer Sound and its foreign subsidiaries and independent contractors are all U.S. persons for purposes of OFAC compliance and liability.

An "*SDN*" or "*Specially Designated National*" is a person or entity OFAC has identified and listed on the SDN List as part of its enforcement efforts. OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked and U.S. persons, including Meyer Sound, are generally prohibited from dealing with them.

The "*SDN List*" is published on the OFAC website. The list is disseminated in a number of different formats, including fixed field/delimited files that can be integrated into databases. The SDN List is frequently updated. Therefore, Meyer Sound should use the published list on the OFAC website (and its search function) when performing transactional due diligence.

## Sanctions Programs

The following is a list of sanctions programs administered by OFAC. Programs are added, discontinued and changed from time-to-time, so the current status of an OFAC administered program of interest should checked.

1. Comprehensive Sanctions
    a. Cuba
    b. Crimea region of Ukraine
    c. Iran
    d. North Korea
    e. Sudan
    f. Syria
2. Selective Sanctions
    a. Western Balkans Region
    b. Belarus
    c. Burundi
    d. Central African Republic
    e. Democratic Republic of Congo
    f. Iraq
    g. Lebanon
    h. Liberia
    i. Libya
    j. Somalia
    k. Yemen
    l. Venezuela
    m. Zimbabwe

3. Entity/Person-Based Sanctions (comprehensive ban against listed entities/persons)

    a. Specially Designated Nationals (“SDNs”)

    b. Terrorists

    c. Narcotics Traffickers

    d. WMD Proliferators

    e. Transnational Criminal Organizations

    f. Foreign Sanctions Evaders

## Using the SDN List

OFAC publishes an updated SDN List on its website. At the time this policy was published, the web address was http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx. As was stated before, the list is disseminated in a number of different formats, including fixed field/delimited files that can be integrated into databases.

The most useful function of the online SDN List is its search function, which is located at http://sdnsearch.ofac.treas.gov/. This is an OFAC maintained, web-based search service that is free, easy to use, and very effective. Employees, when asked to cross-check names against the SDN List, should visit this page and perform queries. This web-based service allows employees to search within some or all of the sanctions programs by name, address, city, state, country, and ID number.

In addition to returning results that are exact matches (when the match threshold slider bar is set to 100%), SDN Search can also provide a broader set of results using fuzzy logic. This logic uses character and string matching as well as phonetic matching. Currently, only the name field of SDN Search invokes fuzzy logic when the tool is run. The other fields on the tool use character matching logic.

Fuzzy logic is a powerful and useful tool for SDN List name searches. It is a function that allows for crosschecking the list against imperfect spellings and phonetic matching of names. The fuzzy logic score field indicates the similarity between the name entered and resulting matches on the SDN List. It is calculated using two matching logic algorithms: one based upon phonetics, and a second based upon the similarity of the characters in the two strings. A score of 100 indicates an exact match, while lower scores indicate potential matches.

When using fuzzy logic, the minimum name score field limits the number of names returned by the search. A value of 100 will return only names that exactly match the characters entered into the name field. A value of 50 will return all names that are deemed to be 50% similar based upon the matching logic of the search tool. By lowering the match threshold the system will return a broader result set.

The SDN List also provides any known “weak aliases” (or AKAs) of an SDN. A “weak AKA” is a term for a relatively broad or generic alias that may generate a large volume of false hits. Weak AKAs include nicknames, noms-de-guerre, and unusually common acronyms. OFAC includes these AKAs because, based on information available to it, the sanctions targets refer to themselves, or are referred to, by these names. As a result, these AKAs may be useful for identification purposes, particularly in confirming a possible “hit” or “match” triggered by other identifier information. Realizing,

however, the large number of false hits that these names may generate, OFAC qualitatively distinguishes them from other AKAs by designating them as weak. Accordingly, hits that only occur because of the AKAs should be given less than weight than the other identifying information. However, if there is correlation of the AKA with the other information, it may indicate an actual match.

Weak AKAs appear differently depending on which file format of the SDN List is utilized. For example, in the TXT and PDF versions of the SDN List, weak AKAs are encapsulated in double-quotes within the AKA listing:

> ALLANE, Hacene (a.k.a. ABDELHAY, al-Sheikh; a.k.a. AHCENE, Cheib; a.k.a. **"ABU AL-FOUTOUH"**; a.k.a. **"BOULAHIA"**; a.k.a. **"HASSAN THE OLD"**); DOB 17 Jan 1941; POB El Menea, Algeria (individual) [SDGT]

Reading an entry on the SDN List may be confusing, but the entry contains a lot of useful information for due diligence purposes. "Weak aliases" have already been explained. The other information on an SDN List entry includes: (1) strong aliases (ones not put in double quotations); (2) date of birth (if known); (3) known addresses or residences; (4) an indication of whether the person is an individual, entity, aircraft, or vessel; (5) citizenship or nationality; and (6) the sanctions programs under which the person was listed in brackets.

For reference purposes, the various sanctions programs are identified in the SDN List as the following bracketed entries:

[BALKANS]: Western Balkans Stabilization Regulations, 31 C.F.R. part 588; Executive Order 13304, 68 FR 32315; [BELARUS]: Executive Order 13405, 71 FR 35485; [BPI-PA]: Blocked Pending Investigation, Patriot Act; [BPI-SDNTK]: Blocked Pending Investigation, Foreign Narcotics Kingpin Sanctions Regulations, 31 C.F.R. part 598; [BURMA]: Burmese Sanctions Regulations, 31 C.F.R. part 537; Executive Order 13448, 72 FR 60223; Executive Order 13464, 73 FR 24491; [COTED]: Cote d'Ivoire Sanctions Regulations, 31 C.F.R. part 543; [CUBA]: Cuban Assets Control Regulations, 31 C.F.R. part 515; [DARFUR]: Darfur Sanctions Regulations, 31 C.F.R. part 546; [DPRK]: Executive Order 13551; [DRCONGO]: Democratic Republic of the Congo Sanctions Regulations, 31 C.F.R. part 547; [EO13622]: Executive Order 13622; [FSE-IR]: Foreign Sanctions Evaders - Iran, Executive Order 13608; [FSE-SY]: Foreign Sanctions Evaders - Syria, Executive Order 13608; [FSE-SDGT]: Foreign Sanctions Evaders - Terrorism, Executive Order 13608; [FSE-WMD]: Foreign Sanctions Evaders – Terrorism, Executive Order 13608; [FTO]: Foreign Terrorist Organizations Sanctions Regulations, 31 C.F.R. part 597; [HRIT-SY]: Executive Order 13606 - Syria; [HRIT-IR]: Executive Order 13606 - Iran; [IFSR]: Iranian Financial Sanctions Regulations, 31 CFR

part 561; [IRAN]: Iranian Transactions Regulations, 31 CFR part 560; [IRAN-HR]: Executive Order 13553; [IRAN-TRA]: Executive Order 13628; [IRAQ2]: Executive Order 13315, 68 FR 52315; Executive Order 13350, 69 FR 46055; [IRAQ3]: Executive Order 13438, 72 FR 39719; [IRGC]: Iranian Financial Sanctions Regulations, 31 CFR Part 561 [ISA]: Iran Sanctions Act, Executive Order 13574; [JADE]: Pub. L. 110-286, 122 Stat. 2632; [LEBANON]: Executive Order 13441, 72 FR 43499; [LIBERIA]: Former Liberian Regime of Charles Taylor Sanctions Regulations, 31 C.F.R. part 593; [LIBYA2]: Libyan Sanctions, 31 C.F.R. part 570; [MAGNIT]: Sergei Magnitsky Rule of Law Accountability Act of 2012; [NDAA]: National Defense Authorization Act for Fiscal Year 2012 (PL 112-158); [NPWMD]: Weapons of Mass Destruction Proliferators Sanctions Regulations, 31 C.F.R. part 544; [SDGT]: Global Terrorism Sanctions Regulations, 31 C.F.R. part 594; [SDNT]: Narcotics Trafficking Sanctions Regulations, 31 C.F.R. part 536; [SDNTK]: Foreign Narcotics Kingpin Sanctions Regulations, 31 C.F.R. part 598; [SDT]: Terrorism Sanctions Regulations, 31 C.F.R. part 595; [SOMALIA]: Somalia Sanctions Regulations, 31 C.F.R. part 551;[SUDAN]: Sudanese Sanctions Regulations, 31 C.F.R. part 538; [SYRIA]: Syrian Sanctions Regulations, 31 C.F.R. part 542; Executive Order 13399, 71 FR 25059; Executive Order 13460, 73 FR 8991;[TCO]: Transnational Criminal Organizations Executive Order 13581; [ZIMBABWE]: Zimbabwe Sanctions Regulations, 31 C.F.R. part 541; Executive Order 13391, 70 FR 71201; Executive Order 13469, 73 FR 43841; and [561List]: Informational tag indicating that this designation is also listed on the List of Foreign Financial Institutions Subject to Part 561 (the "Part 561 List"); North Korean Sanctions, Executive Orders 13466, 131551, 13570, 13687 and 13722; Ukraine/Russia-Related Sanctions Program, Executive Order 13685 related to prohibition of the exportation and importation of goods, services or technology to or from the Crimea region of Ukraine.

## General Due Diligence Procedures

The following provides an overview of the transactional due diligence that underlie special compliance protocols adopted by Meyer Sound for complying with OFAC sanctions.

*Fact Gathering*

The first phase of transactional due diligence is fact gathering. Fact gathering for OFAC compliance focuses on four primary lines of inquiry:

1. What?
2. Where?
3. Who?
4. Why?

These four questions should be addressed at some level before undertaking any foreign or potentially foreign transaction. Getting answers to these questions may in some cases require an employee to do some extra legwork beyond following the company's OFAC compliance protocols (e.g. make phone calls, ask follow up questions, visit websites for verification, communicate with others, liaise with trusted overseas partners to obtain corroborating information etc.). Additional investigative work may be needed to analyze a transaction and make a well informed judgment about it.

What**?**

This inquiry simply relates to what Meyer Sound is exporting (or possibly importing) in a given transaction. Are they products, services (such as technical support or training) or technology? Knowing the subject matter of the transaction helps determine what specific analysis will be required when assessing the transaction.

Where?

This inquiry is intended to determine whether any of the country-based sanctions programs will be implicated (e.g., Iran, Syria, Sudan, etc.). Meyer Sound's OFAC compliance protocols are intended to prevent sales to sanctioned countries.

Who?

This inquiry is to identify the parties in a chain of a proposed transaction, provision of service, or sale, in order to determine if any party to the transaction appears on OFAC's SDN List. Meyer Sound must be able to positively identify the dealer, distributor, and, to the extent possible, the end-user in each transaction. In appropriate circumstances, freight forwarders, shippers, insurers, and other intermediaries in the transactional chain may need to be identified. Again, Meyer Sound's OFAC compliance protocols are designed to obtain this sort of information and to make the necessary SDN checks to determine if any party is subject to OFAC sanctions.

In general, more scrutiny should be applied to transactions with lesser known customers, end-users, intermediaries, dealers, and distributors. However, trusted parties should still be asked questions to determine whether the company's products are ending up in sanctioned nations or in the possession of SDNs. As appropriate, parties, after being identified will be cross-checked against the SDN List for hits or matches.

Complete information about the parties facilitate SDN checks. Complete identifying information for individuals includes: (1) full legal name; (2) nationality or citizenship; (3) address; (4) employer; and (5) whether the person is an agent or principal.

Complete identifying information for entities includes: (1) name; (2) country of formation and/or registry; (3) main company address; (4) satellite office addresses; (5) full name and national registry of parent company; and (6) names of any subsidiaries.

The transactional chain also includes the identities of any account holders, banks and/or financial institutions whose accounts will be used to transfer any funds related to the transaction. As appropriate based on the circumstances of a transaction, employees should identify the banks and/or financial institutions that will be involved in the transaction, if not already known. If appropriate, these persons, entities, and financial institutions should be crosschecked against the SDN List and OFAC's country based sanctions programs. If the bank is a well-known financial institution (e.g., Bank of America, Wells Fargo, etc.) in a non-sanctioned country or low risk region there is no need to crosscheck the institution.

Why?

Asking why a dealer, distributor, end-user, or other customer needs the product helps uncover additional information such as the identity of previously undisclosed parties, where the products will end up, and the purpose for acquiring such goods.

*Screening*

Once the answers to the above questions are known, the transaction is screened, first as to potential violations on country specific sanctions and second as to potential violations of SDN sanctions.

Iran, Cuba, Crimea, North Korea, Sudan, and Syria

First, all transactions, directly or indirectly, involving Iran, Cuba, the Crimea region of Ukraine, North Korea, Sudan, and Syria should be immediately cancelled and/or not pursued. For example, if the goods or services will be sent or received by a person in any one of the countries or by a person who ordinarily resides in any one of those the countries, the transaction should not be pursued. Nor should the transaction be pursued if there is reason to believe that the goods or services will eventually end up in one of those countries.

SDN Searches

Generally, customers and clients should, as appropriate, be checked against the SDN List based on all available information. SDN searches are conducted on OFAC's web-based SDN List at http://sdnsearch.ofac.treas.gov/, and are provided for in the company's OFAC compliance protocols. The following is an overview of how to approach an SDN search:

(1) Compare the name in the transactions with the name on the SDN List. Is the name in your transaction an individual while the name on the SDN List is a vessel, organization, or company (or vice-versa)? If yes, you do not have a valid match. If no, then you may have a valid match and you should go on to #2.

(2) Now you should check to see how much of the SDN's name is matching against the name in the proposed transaction. Is just one of two or more names matching (i.e., just the last name)? If yes, you do not have a valid match. If no, then you may have a valid match and should go on to #3.

(3) Compare the complete SDN entry with all of the information you have on the name matching in your transaction (i.e., the "What, Where, Who, Why" information). An SDN entry often will have a full name, address, nationality, passport, tax ID or cellular number, place of birth, date of birth, former names and aliases. The more matches there are, the more likely it is that there is a valid match. However, if you are missing information and cannot corroborate the matching name with any other identifiers, then you must go back and get more information. Ultimately, you need to reasonably be able to determine that the person the company may transact with is or isn't the person that is

hitting on the list. Without a reasonable basis to conclude one way or the other, the transaction should not be pursued.

And finally, if there is a match and several of the identifiers match or are similar you likely have a valid match. The transaction should be cancelled and/or abandoned and you should summarize your findings in a written report. This report will assist senior management determine whether to report the match to OFAC. Consultation with counsel may be necessary prior to contacting OFAC.

## Document Retention Policy

Meyer Sound and its employees shall maintain complete records of every international transaction for at least ***five years***. OFAC regulations require "every person engaging in any transaction subject to the provisions of" economic sanctions to "keep a full and accurate record of each such transaction engaged in, regardless of whether such transaction is effected pursuant to a license or otherwise," for at least five years. 31 C.F.R. § 501.601.

Maintaining complete records means keeping a true and legible copy of all sales, service, distribution, marketing, partnership, delivery or supply contracts or agreements, requests for proposals, and bid information or correspondence between Meyer Sound, its affiliates, branches, offices, agent, representatives, or distributors and any individual or entity.

Meyer Sound and its employees should also retain for five years all other documents arising from international or foreign transactions, such as invoices, air waybills, shipping documents, financing and payment information, wire requests, and correspondence (including but not limited to electronic mail and facsimile transmissions).

Document retention is critically important to Meyer Sound's overall compliance efforts. Not only is a failure to maintain complete records in and of itself a regulatory violation, maintaining such records will assist the company comply with an OFAC subpoena if one was ever issued. Maintaining complete records will also help Meyer Sound conduct its own internal investigations of possible violations.

## Facilitation and Brokering Services Prohibited

Meyer Sound and its employees, dealers, distributors, subsidiaries, and independent contractors (collectively, Meyer Sound) should be careful not to inadvertently violate the sanctions by facilitating or brokering a transaction that would be prohibited if conducted by Meyer Sound.

Specifically, Meyer Sound cannot facilitate, transport, swap, approve, finance, or broker any transaction or activity if such transaction or activity would be prohibited if performed by the Meyer Sound. This prohibition also includes referrals to a foreign person of purchase orders, requests for bids, or similar business opportunities involving any nation subject to comprehensive sanctions or any persons designated on the SDN List.

For example, if someone working for Meyer Sound introduces a person from Iran to a foreign person for the purpose of facilitating or fostering a business opportunity, that employee would be in violation of the "facilitation" clause of the sanctions. Therefore, employees should not help persons targeted by sanctions or persons living in countries targeted by sanctions secure business opportunities, referrals, or business relationships.

Facilitation also prohibits Meyer Sound from changing its operating policies and procedures of a particular affiliate with the specific purpose of facilitating transactions that would be prohibited by the sanctions regulations if performed by a United States person or from the United States.

## Possible Violations, Internal Investigations, and Self-Reporting

If an employee realizes that Meyer Sound performed a transaction prohibited by the sanctions, that employee must contact the Executive Vice President or her designee (collectively "EVP") immediately. Violations that occurred more than five years ago are beyond the statute of limitations. Although no liability will result from such time-barred violations, investigating and learning from such violations is important because they will help maintain a culture of compliance and vigilance in the company.

Upon being notified of a possible violation the EVP should request the production of all retained documents and information related to the questionable transaction. The EVP should then contact legal counsel to analyze the breadth and scope of liability derived from that transaction. Additionally, it is of critical importance to determine whether the violation is ongoing or historic. If the violation is ongoing, all efforts must be made to cease the transaction as quickly as possible. Knowing about an ongoing violation and not stopping it can be used as evidence of willfulness. Willfulness can significantly increase the potential penalties, including imprisonment.

Employees directly and indirectly involved with the possible violation should be interviewed. These interviews should complement and add insight to the documentary evidence that Meyer Sound has already retained about the transaction.

Through this Compliance Policy, Meyer Sound recognizes that self-reporting possible violations to OFAC is usually the most beneficial course of action. If Meyer Sound, upon consulting with counsel, determines that it will self-report the possible violation, it will shortly thereafter file a brief letter with OFAC stating that it may have identified a possible violation. A brief description of the violation will be provided to OFAC in that initial letter. This letter will also inform OFAC that the company is performing an internal investigation and will provide OFAC with its findings when the investigation is concluded.

The company's subsequent filing with OFAC should include the conclusions and the findings of the internal investigation. OFAC should also be given a copy of all relevant documents related to the transaction. The filing should also analyze the potential violation in light of the OFAC Enforcement Guidelines. And lastly, this filing should also discuss any applicable mitigating factors, legal considerations, and policy considerations.

OFAC encourages companies to voluntarily disclose a past violation. Self-disclosure itself is considered a mitigating factor by OFAC in Civil Penalty proceedings. Not only does self-reporting demonstrate the company's willingness to cooperate, it also assists the agency in its overall enforcement function.

Although OFAC does not have a formal “amnesty” program, the OFAC Enforcement Guidelines recommend that those who voluntarily self-disclose received significantly reduced civil penalties.

For example, in non-egregious cases a company that self-discloses will be only be fined one-half of the transaction value (capped at $125,000 or $32,500 per violation depending on the program). In the same non-egregious case but without a self-disclosure, the company will be penalized according to the applicable schedule amount (capped at $250,000 or $65,000 per violation depending on the program)

In an egregious case with a self-disclosure, a company will be subject to only one-half of the applicable statutory maximum. However, the same egregious case without a self-disclosure subjects the company to the applicable statutory maximum of $250,000 or twice the amount of each underlying transaction, whichever is higher, for each violation.