ACSS
ASSOCIATION OF CERTIFIED SANCTIONS SPECIALISTS

Certified Sanctions Specialist (CSS)

Exam Preparation Guide

May 2020
Version 11

Association of Certified Sanctions Specialists (ACSS)
7950 NW 53rd Street Suite 337
Miami, FL 33166
Phone: +1 305 433 7187
helpdesk@sanctionsassociation.org
www.sanctionsassociation.org

Table of Contents

Contributions

ACSS wishes to thank those who contributed to the development of the CSS and this Study Guide.

Study Guide

Contributing Author: Scott Nance, Langley Compliance Consulting LLC
Editor: Saskia Rietbroek, CSS, Executive Director, Association of Certified Sanctions Specialists (ACSS)

Certified Sanctions Specialist (CSS) – Certification Task Force

The following ACSS members participated in the different phases of the CSS exam development process, including the Job Analysis, Item Writing and Cut Score Workshops.

ACSS thanks them for their support!

FIRST	LAST	JOB TITLE	ORGANIZATION
Ahmed	Abul-Ola	Senior Officer, Anti Money Laundering	The National Commercial Bank
Alecia	Alison	BSA/AML Compliance Officer	Home Credit U.S.
Theone	Alleyne	Sr. Managing Consultant Risk & Compliance Practice	IBM
Ramanuj	Basu	Senior Manager	Clearbanc
Matt	Bell	Senior Managing Director, Global Practice Co-Leader Export Controls and Sanctions Practice	FTI Consulting
Stefano	Boezio	Consultant	Oliver Wyman
Ann	Broeker	Assistant General Counsel	Moody's Corporation
Tatjana	Dobrovolny	Senior Expert Compliance Programs and Systems Solutions	Raiffeisen Bank International AG
Josue	Garcia	Global Legal-Ethics & Corporate Compliance, Sr. Manager	Carnival
Thorsten	Güldner-Bervoets	Sanctions	Raiffeisenbank International
Tyler	Hand	Chief Compliance Officer	Western Union
Glenda	Juliano	Sr. AML & Trade Control Analyst International Global Risk Control	Franklin Templeton
Heidi	Kinkartz	Director, Global Sanctions	Scotiabank
Leslie	Kuester	Head, Global Sanctions Strategy	Western Union

FIRST	LAST	JOB TITLE	ORGANIZATION
Marsha	Mitts	Trade Center of Excellence - Sanctions Manager Law Security & Public Policy	Caterpillar Inc
Max	Lerner	Vice President, Global Head Sanctions Compliance	State Street Corporation
Scott	Nance	Attorney	Langley Compliance Consulting LLC
Alina	Nedea		EU Commission
Ben	Omorogbe	VP & Group General Counsel | Legal	Travelers Insurance
Francisco	Rapp	Chief Sanctions Officer	Citi
Eric	Rudolph	Director	FTI Consulting
Simon	Ring	Global Head - Regulatory Technologies	Polestar
Jacqueline	Santos	AML Sanctions Director Senior Vice President Enterprise AML/BSA and Sanctions	PNC
Philip	Schell		United Nations
Hera	Smith	Senior Compliance Officer, Sanctions and Embargo	Danske Bank
Clay	Stevenson	Managing Director, Head of Sanctions & Embargoes, Americas	Deutsche Bank
Samantha	Sultoon		Atlantic Council
Arlene	Swanson	Director, Corporate Compliance Sanctions Compliance	Nationwide
Inna	Tsimermann	Chief International Trade Counsel	Gallagher
Amber	Vitale	Managing Director, Forensics & Litigation Consulting	FTI Consulting
Peter	Weiss	Sr. Sanctions Manager | Enterprise AML	BMO
Robert	Werner	Founder and CEO	Green River Hollow Consulting

INTRODUCTION

Association of Certified Sanctions Specialists (ACSS)
7950 NW 53rd Street Suite 337
Miami, FL 33166
Phone: +1 305 433 7187
helpdesk@sanctionsassociation.org
www.sanctionsassociation.org

INTRODUCTION

How to Use this ACSS Examination Preparation Guide

This study guide is designed to be a companion to the “CSS Exam Preparation Virtual Classes” and a comprehensive self-paced exam preparation tool.

The guide is divided into eleven primary sections to better facilitate the study process:

I. Introduction
II. Sanctions Regime Types, Goals, Prohibitions and Effects
III. Sanctions Imposers and Targets
IV. Sanctions Evasion: Typologies and Schemes
V. Essential Components of a Risk-Based Sanctions Compliance Program in Different Industry Settings
VI. Role of Technology and List Screening
VII. Other Operational Issues
VIII. Enforcement and Conducting/Supporting Investigations into Sanctions Violations
IX. Reference Material and Reading List
X. Glossary
XI. Practice Questions

The CSS study guide uses icons to emphasize key points, definitions and information, to point out case studies and examples and to direct the reader to the reference section for additional information.

The lightbulb can be found next to key points and definitions

The scale and gavel indicates a case study or scenario example

The books direct the reader to the reference section for more information

This study guide was designed to assist candidates in preparing for the CSS Certification Examination. It includes an overview of the test development process, test taking techniques and reference materials for topics included in the content outline for the examination. This study guide is not meant to address all possible conditions or questions, nor does it represent a comprehensive preparation for the examination. The editors of this examination study guide and ACSS do not have knowledge of specific examination questions. While this guide is intended to assist candidates in preparing for the examination, they are expected to prepare for the examination through self-study.

About ACSS

The Association of Certified Sanctions Specialists (ACSS) is a professional membership body for sanctions professionals worldwide. It was formed to advance sanctions compliance by supporting the professional development of the individuals who lead those efforts.

The goal of ACSS is to:

- Serve the professional interests of its members by delivering high quality services and promoting the interests of the profession
- Provide professional qualifications and set standards for sanctions practitioners
- Be an authoritative and respected voice promoting sanctions compliance
- Enhance the careers of sanctions professionals worldwide

See http://www.sanctionsassociation.org

Advisory Board

Guided by an Advisory Board of distinguished experts, ACSS is dedicated to providing its members top quality education, career development programs, and other membership benefits – including information exchange and peer networking – to help in advancing their skills.

Through professional certification and qualifications, ACSS members stand out as leaders in the field.

ACSS Advisory Board Members:

Clay Stevenson
Advisory Board Chair
Founder
CHS Sanctions Advisory

Matt Bell
Senior Managing Director
FTI Consulting

Ms. (Dipl. Ing.) Tatjana Dobrovolny
Senior Expert Compliance Programs and Systems Solutions
Raiffeisen Bank International Group

Brian Grant
Global Head of Sanctions Compliance
Mitsubishi UFJ Financial Group (MUFG)

Pinar Gungoren Chedru
Global Head of Embargoes and Sanctions Compliance
Societe Generale

Heidi Kinkartz B.A., LL.B., CAMS
Director Global Sanctions
Scotiabank

Francisco Rapp
Chief Compliance Officer, Sanctions and Anti-Bribery
Citi

Robert Walsh
Deputy Chief Compliance Officer and Global Financial Crime Officer
AXA Group

Karen Robertson
Global Trade Compliance Officer
Uber Technologies, Inc.

Jacqueline Santos
Senior Vice President Enterprise Compliance Bank Secrecy/Anti-Money Laundering and Sanctions
PNC Bank

Todd Willis
Global Trade Advisor
Caterpillar, Inc.

Robert Werner
Founder
GRH Consulting

ACSS Member Resources and Training

What are the core benefits of joining the Association of Certified Sanctions Specialists (ACSS)? As an ACSS Member, you will gain access to:

CSS Certification Exam, which allows sanctions professionals the opportunity to earn credentials as a Certified Sanctions Specialist, or CSS. The credential will provide ACSS members with a powerful career advantage and their employers and clients the comfort of knowing that he or she has met high standards of knowledge and training. The CSS credential will test members' skills in sanctions compliance, export control duties, listing matching, consulting, investigating, and more!

Education and Online Certificate Programs, which provide sanctions professionals to gain expertise in important sanctions topics., such as OFAC Essentials, EU Restrictive Measures and Anti-Bribery Essentials.

Live and On-demand Webinars, which include 25+ LIVE webinars per year, where attendees can ask real-time questions during expert-led sessions and even earn CE/CLE credits. ACSS Members also have the unique opportunity to browse our archive of on-demand webinars by logging into our online Learning Management System (LMS).

Interactive Sanctions Map, an interactive tool with an overview of sanctions in place against countries around the world. The Map focuses on sanctions imposed by the U.S. (OFAC), E.U., U.K., U.N., and Canada. Find out what specific sanctions are in place against a country by simply clicking on that particular country!

Sanctions Enforcement Actions Database, where you can search, browse, and download 900+ OFAC enforcement cases. The database is searchable by country, year, and industry.

Official Sanctions Guidance Library, where you can find guidance provided by government agencies, international institutions, and universities about how to best implement sanctions in your country.

Sanctions Service Providers Directory, an invaluable resource for members looking to contact software vendors, consultants, law firms and other providers specializing in the sanctions field.

Task Forces, where you can join up with your colleagues to shed light on important sanctions topics and connect with others in the sanctions community. These Task Forces are only available to ACSS Members.

Online Certificate Courses

In order to meet the need for more in-depth training on certain sanctions-related topics and mitigate the risk of costly sanctions violations, ACSS developed several online sanctions training courses, which teaches vital principles and background all sanctions compliance staff should understand.

The online Certificate Courses are 7-part courses, consisting of approximately 6 to 7 training hours, across 4 weeks. The courses are delivered in an online format.

ACSS offers the following online Certificate Courses:

- OFAC Essentials
- EU Restrictive Measures Essentials
- Anti-Bribery Essentials

For more information and updates: https://sanctionsassociation.org/certificates/

CSS Certification

The Association of Certified Sanctions Specialists offers an examination that addresses knowledge and skills common to all sanctions professionals in varied employment settings, including financial institutions, international corporations, law firms, consulting companies, government, and other trades and businesses.

The objective of the certification program is to set the standard for the sanctions profession, and to make Certified Sanctions Specialists (CSS) widely recognized as trained and credentialed specialists in the sanctions field. It is a multiple-choice, proctored exam that can be taken in testing centers across the globe.

Why this Certification?

Career opportunities abound for the sanctions specialists, but the days are over that just anyone can fulfil that role. Especially in these days, the “consumer” of the services of a compliance officer or other sanctions expert has become more vigilant, demanding quality. This demand is exacerbated by the media’s constant attention to sanctions issues arising at financial institutions, or international businesses. Certification of the sanctions professional in organizations that are vulnerable to the problem is designed to meet this consumer concern.

Benefits of Certification

- Pride
- Growth
- Employment
- Financial Rewards
- Reputation
- Achievement

Testing Centers

We have partnered with a world leader in brick and mortar testing centers. We also offer secure online proctoring.

CLOSE TO YOU

Over 5,100 test centers in over 190 countries. Located at over 2,560 different cities.

FLEXIBILITY

A scheduling portal finds the center nearest to you and helps you schedule the date and time of the test.

COMMUNICATION

Get support, reminders, and directions to the test center.

HELP

Our testing centers are started with personnel that will guide through the identification process and testing protocols.

What is on the exam?

The exam will focus on various aspects of the sanctions subject. A job analysis will determine the content and the importance of each knowledge area for the specialists in the field. The certification exam will be tailored to international best practices and basic frameworks for sanctions efforts around the world.

I. Sanctions Regime Types, Goals, Prohibitions and Effects
II. Sanctions Imposers and Targets
III. Sanctions Evasion: Typologies and Schemes
IV. Essential Components of a Risk-Based Sanctions Compliance Program in Different Industry Settings
V. Role of Technology and List Screening

VI. Other Operational Issues Contributing to an Effective and Efficient Sanctions Compliance Program
VII. Enforcement and Conducting or Supporting Investigations into Sanctions Violations

Administration of the exam

Since ACSS members reside worldwide, ACSS uses a computerized exam. ACSS offers the exam throughout the year in brick and mortar testing centers, plus through online proctoring. Requirements to sit for the exam include the completion of an ACSS exam application and payment of an application fee. For more information see here: https://sanctionsassociation.org/css-process/.

Who can take the exam?

ACSS Certification eligibility is based on a points system. Candidates who wish to take the CSS Examination must have a minimum of 40 qualifying credits based on education, other professional certification, and professional experience in the sanctions field (see below), in addition to providing 3 references.

Further, you must be an active member of ACSS in order to sit for the exam.

Point system:

I. Education:
   a. Associate Degree: 10 credits
   b. Bachelor's Degree: 20 credits
   c. Master's Degree/PhD/JD or equivalent: 30 credits

II. Professional experience:
   a. Each year of full-time experience in sanctions or related duties.
   b. Professional experience is limited to 3 years: 10 credits per year

III. Training:
   a. Professional Certification – CPA, CPP, CRCM, CAFP, CFE, CAMS, CGSS, ETCI ECoP, Finra Series, etc: 10 credits per certification.
   b. Attendance at a course / seminar / webinar / conference / training / certificate courses or educational session on the topic of sanctions, trade compliance or export controls or related subjects (includes internal training, external training, government agency training) – 1 credit per hour.

For more information, visit: https://sanctionsassociation.org/

SANCTIONS REGIME TYPES, GOALS, PROHIBITIONS AND EFFECTS

Sanctions: Definitions and Objectives

"{W}e must develop alternatives to violence that are tough enough to actually change behavior — for if we want a lasting peace, then the words of the international community must mean something. Those regimes that break the rules must be held accountable. Sanctions must exact a real price. Intransigence must be met with increased pressure — and such pressure exists only when the world stands together as one."

Barack Obama (Nobel Peace Prize Acceptance Speech, Oslo, 9 December 2009)

What Are Sanctions?

Sanctions are financial, physical, and other measures taken to prevent certain types of activities or to influence the behavior of countries, groups, or individuals. Economic sanctions have traditionally been defined as the "deliberate, government-inspired withdrawal, or threat of withdrawal, of customary trade and financial relations with a target country in an effort to change that country's policies."[1] In other words, economic sanctions are legal measures that typically restrict or prohibit trade and financial transactions with specified targets. Sanctions may also allow certain types of behavior, such as investment in a sanctioned country, but require that it be reported. A key point is that sanctions are legal measures; they have the force of law, and failure to comply with them can give rise to potentially severe penalties.

One important aspect of economic sanctions is that they are to a large extent self-enforced, as their effectiveness depends primarily on voluntary compliance. In this way they differ from military measures, such as naval blockades. Sanctions are also different from other trade measures, although they may shade into one another. The imposition of import or export duties or quotas, for example, are not generally considered to be economic sanctions. In general, economic sanctions are used to accomplish political rather than economic goals, although the difference between the two can be subtle.

Throughout this guide, the country imposing sanctions is identified as the sanctioning country. The country that is the target of the sanctions is referred to as the target country.

Sanctions Objectives

Sanctions may have several different objectives. These include:

- To deny resources to the target, with the aim of making certain activities, such as terrorism or narcotics trafficking, impossible;
- To persuade or compel the target to change its practices

---

[1] Gary Hufbauer & Barbara Oegg, A Short Survey of Economic Sanctions, INST. FOR INT'L ECON. (Aug. 2001), http://www.ciaonet.org/casestudy/hug01/.

- To penalize the target for its practices
- To make a symbolic political statement, either to domestic political constituencies or to the global community as a whole

These are largely political goals, and the imposition and administration of sanctions is inherently political. This means that sanctions can change, often quite rapidly, in response to political events. There is a tendency for sanctions, once imposed, to remain in place, whether or not they have proven effective in accomplishing their goals.

The History of Sanctions

The use of economic sanctions as a formal instrument of policy goes back to at least 432 B.C.. In that year, Pericles, the Athenian statesman, proposed a ban that would prohibit citizens of Megara, a nearby Greek city-state, from harbors and markets throughout the Athenian empire. In this respect, the Megarian decree resembled a modern economic embargo.

Even "targeted" sanctions and secondary sanctions have a long history. Between 232 and 225 B.C., Rome prohibited anyone (including non-Romans) from buying gold or silver from or selling it to the Gauls. A more recent example occurred in 1531, when Zurich and other Protestant cantons in Switzerland prohibited the sale of flour, salt, iron, and wine to Catholic cantons, on the grounds that the latter had violated their treaty obligations to respect the rights of minority Protestants.

The history of economic sanctions in the United States – probably the greatest user of sanctions – goes back to the War of Independence. The United Kingdom launched a naval blockade of the rebellious colonies; in response, the Continental Congress banned all ships from Britain and its dominions from U.S. ports. After independence, the United States continued to use sanctions as an instrument of policy preferable to military force. In 1806, the United States banned the importation of a range of goods from Great Britain. In 1807, it enacted a general embargo on foreign trade in an attempt to put economic pressure on Great Britain and Napoleonic France by denying them both exports to and imports form the United States. The embargo backfired, causing almost immediate damage to the American economy, and was revoked less than two years later.

U.S. sanctions began to assume their current form during World War I, when the United States seized and froze (and in some cases sold off) assets belonging to the German government and German companies. The most famous example is Bayer aspirin. Great Britain applied similar measures in conjunction with its naval blockade of Germany during the war.

A major development after World War I was the emergence of multilateral sanctions. The Covenant founding the League of Nations specifically authorized its members to use economic sanctions against countries committing military aggression, although such sanctions were in fact only weakly applied. This concept was carried forward and expanded with the United Nations, which has employed sanctions much more widely and, arguably, effectively.

The key principle of sanctions has been that they allow countries to take action without resorting to military force. Not surprisingly, the use of sanctions may under some circumstances exacerbate rather than reduce tensions. The U.S. embargo of exports of oil and scrap metal to Japan in response to Japan's invasion of China, for example, is often given as one of the reasons for the Japanese attack at Pearl Harbor.

Since World War II, sanctions have become increasingly common, and increasingly complicated. Over time, sanctions have tended to become more focused and targeted. Despite doubts over their efficacy, it is likely that the use and scope of sanctions will only expand in the near term.

Sanctions Regimes

Sanctions are usually imposed by countries, although, as discussed below, they may be imposed by international organizations as well. Sanctions may be imposed unilaterally, by a single country, or multilaterally, as is the case with sanctions imposed by the United Nations. Countries may impose sanctions individually, but in coordination and cooperation with allies, as happened with the U.S. and EU sanctions against Russia following events in Ukraine in 2015.

Sanctions are imposed through legal acts. Depending on the country, these may take the form of laws, regulations, executive proclamations, administrative guidance, and administrative and judicial decisions. A country's sanctions laws will cover a number of topics, including what types of sanctions are applied; who they apply to (sanctions targets); who must comply with them (sanctions subjects); what the penalties for non-compliance are; and who administers and enforces the sanctions. The totality of a country's sanctions laws, addressing all of these topics, are known as a sanctions regime. The set of sanctions targeting individual countries or categories (such as terrorists or narcotics dealers) are commonly called sanctions programs.

Imposers of Sanctions

Sanctions can be imposed by any level of government. Sanctions imposed by federal governments apply throughout the country. In addition, subsidiary levels of government, such as the states in the United States, may impose additional sanctions, but these will apply only to the state itself. In the European Union, sanctions can be imposed at both the Union and the national level. Member states must comply with all Union-level sanctions, but can also impose their own sanctions.

International organizations also impose sanctions. The most obvious example is the United Nations. As discussed below, the UN cannot require its member states to comply with UN sanctions, although most do. Other international organizations, such as the World Bank, may impose sanctions as well.

Sanctions Targets

Sanctions typically target either entire countries or, less commonly, regions within a country. Sanctions targeted at countries may apply only to individuals and entities within the country, or to nationals and entities of the country world-wide. Sanctions may also target governments (as opposed to countries themselves).

Comprehensive sanctions employ extensive trade embargoes against the target of sanctions and involve wide-sweeping bans on trade, diplomatic relations, and or other relationships between target and sender. For example, sanctions that prohibit the import or export of goods and services that benefit a country or region.

Targeted or list-based sanctions impose sanctions on specific items or restrictions on a person or on groups of specific people. For example, sanctions that that target specific individuals and entities of a country or region.

Sectoral sanctions: Target a specific industry of a country or region.

Sanctions can apply to named individuals. They may also be imposed against groups or organizations (such as Al Qaida), companies, or other legal or unofficial entities. They may even apply to inanimate objects such as ships or airplanes.

Subjects of Sanctions

The “subjects” of sanctions are those who are required to comply with them. Sanctions generally require compliance by the nationals of the country applying the sanctions. This is true wherever they might be located, even if it is outside the country. Persons physically present in a country must also obey its sanctions, regardless of their citizenship[2]. Entities, such as corporations, organized under the laws of a country must also comply with its sanctions. This is true of their foreign branches as well. Whether or not their foreign subsidiaries must also comply with the sanctions, depends on the sanctions. These types of sanctions are referred to as “direct” or “primary” sanctions.

More rarely, sanctions may impose duties or prohibit conduct by non-nationals, including citizens of other countries or foreign companies operating outside the sanctioning country. These are called “secondary” sanctions. Their validity under international law has been questioned, and the application of sanctions to foreigners may raise political issues as well. At present, the United States is the

[2] This includes the European Union, although the EU is technically an international organization rather than a state.

only country that extensively applies secondary sanctions. Secondary sanctions tend to be somewhat more focused than primary sanctions.

Secondary Sanctions

- Also called "extraterritorial" sanctions;
- Extend power of U.S. law indirectly, to non-U.S. firms;
- May directly prohibit foreign subsidiaries of U.S. companies from engaging in certain types of activity;
- May indirectly target non-U.S. firms by trying to restrict their access to the U.S. market;
- Create risk areas for non-U.S. companies.

Penalties

The duty to comply with sanctions implies that there are penalties for non-compliance. The most common penalties for failing to comply with sanctions are fines. Penalties may also include administrative measures, such as the revocation of licenses or prohibitions against conducting certain activities, such as exporting. Another common "penalty" is the requirement that an organization strengthen its internal sanctions compliance system. In some cases, egregious violations of sanctions requirements may even lead to imprisonment. Finally, violating sanctions may subject the person or organization to designation as a sanctioned party, which can result in the freezing of assets and similar measures.

Administration

What agency or entity administers and enforces the sanctions laws of a country varies by country. Administration may either be assigned to a dedicated agency (as in the United States) or performed by an agency as part of its overall functions (as in Netherlands, for example). Administration and enforcement may be shared or split between various agencies. It is common in particular for different agencies to enforce sanctions and to issue export or import licenses. Given the importance of the banking system in the administration of sanctions (as discussed in Chapter 3 below), bank regulators are usually heavily involved in sanctions administration and enforcement.

Common Types of Sanctions

Sanctions programs may be very broad, or quite targeted. Broad programs that prohibit most are all transactions are often referred to as embargos. Narrow programs, on the other hand, may affect only trade in selected products, such as weapons. While sanctions can vary greatly, they tend to fall into a few common categories.

Prohibitions on Imports

Imports from the target country or region are prohibited. These may include imports of goods, services, and technology. The prohibition may apply only to selected products, or to all imports from the country in question.

Prohibitions or Restrictions on Exports

Prohibitions on exports are another common form of sanctions. There are two common approaches to export prohibitions. One is to prohibit all exporters, although here may be exceptions, such as exports of agricultural products and medicines and medical products. The other is to specify what products are subject to the export ban, with all other exports being permissible.

Exports typically include not just goods, but services and technology as well. Significantly, “services” typically include financial services, which would encompass basically everything banks do, as well as insurance and investment services. Exports of technology include software. As discussed below, the definition of “export” can be very broad, and can reach the transmission of software or information over the Internet, as well as the disclosure of information to nationals of a target country.

Many countries, including the United States, the United Kingdom, and the European Union, impose controls on the exportation of at least some products, typically those with military uses. Export controls are not necessarily sanctions, and may be administered by different agencies. The relationship between the two is discussed in Chapter 6.

Arms Embargos

A prohibition on exports of military items is frequently the first type of sanction imposed against countries. The prohibition will normally cover both arms and items that are used for military purposes. The prohibition may cover either specified items or all goods, services, or technology used by the military. This means that it may be legal to export a product for civilian use, for example, but not for use by the military.

Product-Specific Embargos

General prohibitions on any trade in specified products are another common form of sanctions. The objects of such product-specific embargos include bullion, precious metals, luxury goods, and petroleum.

Prohibitions or Restrictions on Investment

A country may prohibit or limit investment in another country. This typically takes the form of a prohibition on new investment. The prohibition may be general, or may apply only to investment in designated sectors. Such prohibitions do not normally require the liquidation of existing investments. Other restrictions, such as those on the export of financial services or on financial transactions, may severely affect the value of investments in sanctioned countries by limiting the ability to repatriate profits from such investments or to provide funds for repairs or expansion of the investment.

Prohibitions on Financial Transactions

These sanctions may prohibit any type of financial transaction, including processing payments, making loans, or providing any kind of banking, insurance or investment service. Unlike the previous types, prohibitions on financial transactions can apply to individuals and organizations as well as to entire countries.

Prohibition on Providing Economic Resources

At their most sweeping, sanctions may prohibit providing any economic resources to sanctions targets. Economic resources include funds, financial assets, or indeed anything of economic value. This type of sanction is typically applied to individuals or organizations rather than entire countries.

Asset Freezes

Probably the most far-reaching type of sanction is the freezing of assets. The sanctioning country will require that its nationals (including its banks) freeze funds, financial instruments, other assets, and indeed any property belonging to a sanctions target that come under their control. The party freezing the assets must hold them, typically in a separate, designated account, until directed by the government to release them.

The sanctions target continues to own the assets, at least theoretically, but cannot access them. There may be limited exceptions, such as the ability to use frozen funds to pay living expenses. Asset freezes are most commonly directed against individuals and organizations, although they may apply to all property owned by a government.

Sectoral Sanctions

A more recent type of sanctions are sectoral sanctions. These are, as the name implies, directed against specific sectors of the economy of a country, such as the banking, energy, or defense sectors. Sectoral sanctions usually apply only to identified companies. They normally prohibit some, but not all, transactions involving those countries and sectors.

A policy maker would opt for sectoral sanctions rather than blocking or asset freeze prohibitions because some targets are so interconnected to the global economy that a sudden disruption caused by asset free/blocking would have harmful, unintended consequences for the global economy.

Not surprisingly, sectoral sanctions can be very complicated.

Travel and Transit Restrictions

Travel bans are a common type of sanction. They prohibit either named persons or government officials of the target country from entering the country applying the sanctions. There may be exceptions, such as for travel by prohibited government officials to meetings of the UN or other international organizations.

Transit restrictions may prohibit goods from a sanctioned country from passing through the territory of the country imposing the sanctions, or goods from the country imposing sanctions from passing through the territory of the target country, even if they are destined for a non-sanctioned country. Such prohibitions may include goods being carried on ships or planes that stop in a sanctioned country, even if they are not unloaded, but rather continue on their way to a non-sanctioned destination.

Reporting Requirements

In some cases, sanctions do not prohibit transactions with a target country, but require that it be reported. The United States, for example, requires that companies with publicly-traded stock include a statement as to whether they do business with Iran. The theory behind this type of sanctions is that adverse publicity will convince companies not to do business with target countries, even if such business is not technically prohibited.

Circumvention and Facilitation

Not surprisingly, targets of sanctions frequently seek to evade them. The methods for evading sanctions are discussed in detail in Chapter 4. For this reason, attempting to circumvent sanctions is itself prohibited as well.

Facilitation is similar to circumvention. U.S. sanctions programs generally prohibit U.S. persons (wherever located), or non-U.S. persons located in the U.S., from facilitating transactions by foreign persons when those transactions would be prohibited if they were undertaken by U.S. persons themselves.

Examples of “facilitation” include:

- Approving, directing, assisting, supporting, financing or insuring transactions in or with a U.S. sanctioned country;
- Making any purchase for the benefit of a prohibited transaction;
- Negotiating with customers/potential customers in U.S. sanctioned countries;

- Participating in meetings or on calls with nationals of sanctioned countries for the purpose of furthering a prohibited transaction;
- Approving expenses or providing financing related to a prohibited transaction;
- Arranging freight forwarding, customs brokerage services or similar support services related to a prohibited transaction; and
- Negotiating, drafting or reviewing commercial terms/contracts related to a prohibited transaction.
- Types of activities unlikely to be considered by OFAC to constitute unlawful "facilitation" include the following:
- Seeking legal advice regarding the application of U.S. sanctions law to proposed transactions (but beware certain actions taken in furtherance of such advice);
- Transactions carried out independently by a foreign subsidiary, with no involvement by U.S. persons, wherever located, or non-U.S. persons located in the U.S.; or
- Providing back office shared functions by U.S. persons, wherever located, or non-U.S. persons located in the U.S., as long as these activities are purely clerical and do not specifically relate to a prohibited transaction.

Facilitation provisions under U.S. sanctions programs are measures that make it an offense for any U.S. person to approve, facilitate, guarantee or finance any transaction by a foreign person where the transaction by that foreign person would be prohibited if performed by the US person.

Iranian Transactions and Sanctions Regulations, Subpart B, Prohibitions § 560.208 Prohibited facilitation by United States persons of transactions by foreign persons.

Except as otherwise authorized pursuant to this part, and notwithstanding any contract entered into or any license or permit granted prior to May 7, 1995, no United States person, wherever located, may approve, finance, facilitate, or guarantee any transaction by a foreign person where the transaction by that foreign person would be prohibited by this part if performed by a United States person or within the United States.

In summary, U.S. sanctions laws prohibit persons subject to a sanctions regime from assisting a foreign person not subject to that sanctions regime from undertaking an action that would be prohibited if performed by the subject person.

Facilitation is also discussed in Chapter 4.

Exceptions to Sanctions

The precise scope of sanctions differs by country and program. Certain exceptions to sanctions are common around the world, though. These include licenses and exemptions. An action is exempt from sanctions if the sanctions laws simply do not apply to it, or otherwise authorize it. Common exemptions include transactions involving mail and telecommunications, humanitarian donations, family remittances, and payments for overflight privileges. A license, on the other hand, is permission to perform an action that would otherwise be prohibited. Licenses may be specific or general, as discussed below. The distinction between an exemption and a license is not always clear, especially with respect to so-called general licenses.

The following categories of transactions are frequently (though not universally) exempted from sanctions laws:

Post and Telecommunications

Sanctions laws almost always allow communication with a sanctioned country, whether through the mail or via telecommunications. The latter includes e-mail and text messages as well as telephone calls. As part of this exemption, telecommunications companies are commonly allowed to make payments to government authorities in sanctioned countries, as well as to local telecommunications providers. Precisely what is allowed, however, can be complicated. Moreover, the exemption for telecommunications does not necessarily allow investment in the sanctioned country in the equipment needed to carry telecommunications.

Humanitarian Donations

Donations for humanitarian purposes are another frequent exception to sanctions laws. The potential for misuse of this exception is obvious, though, so that donations may be restricted or prohibited under some circumstances. The details of the exemption will specify what types of donations are allowed (such as food, medical supplies, tents and blankets), as well as what types of organizations can receive such donations.

Family Remittances

A less common exemption is for family remittances. The theory is that sanctions should not prevent families from supporting each other. Again, the potential for abuse is obvious. Exceptions for family remittances commonly require that the remittance be for personal rather than commercial use. There may also be a limit on the amount that can be remitted in any one year.

Informational Materials

Sanctions are imposed for political reasons, often with the objective of changing the behavior, or even the government, of a target country. The free flow of information can aid in this process. Accordingly, sanctions regimes and programs frequently exempt informational materials – books, music, movies, and information in general – from the reach of sanctions. Of course, this exception is subject to export controls and other measures, especially where information regarding technology is concerned. In addition, the exception commonly refers to materials already in being; a book co-written by an American and an Iranian, for example, would still violate U.S. sanctions against Iran, despite the general exemption for informational materials.

Travel and Travel Expenses

Sanctions may or may not include a prohibition on travel to sanctioned countries. The United States, for example, prohibits travel by U.S. nationals to Cuba or North Korea, with certain exceptions. Travel to Iran or Syria, on the other hand, is allowed. Where travel is not prohibited, sanctions laws generally include an exemption for travel expenses, with the requirement that the expenses be directly related to travel.

Overflight Payments

Countries generally charge for the right to pass through their airspace. Rerouting flights to avoid sanctioned countries is in many cases simply not practical. For this reason, sanctions laws almost always contain an exemption for overflight payments. This exception also includes the right to pass through the airspace of a sanctioned country.

Agricultural Products

When countries impose sanctions on other countries, it is common for them to insist that their objective is to change the behavior of the government of the country, not to punish the population as a whole. For this reason, sanctions laws commonly exempt agricultural exports (but not necessarily imports). The underlying theory is that food should not be used as a weapon. The laws may provide a broad exemption, or identify in detail which products are or are not exempt. Use of the exemption may also require the exporter to follow certain procedures, including how payment can be made.

Medicine and Medical Products

Medicine and medical products are normally exempted from export prohibitions as well. As with agricultural products, the relevant sanctions program may describe in some detail what products, services, and technology benefit from the exemption.

Licenses

Governments may decide to allow transactions that would otherwise be forbidden by sanctions. This permission normally takes the form of a license. While the details of licensing vary by country, a license typically identifies who may perform the action; exactly what action may be performed (the sale of a particular product, the provision of services, etc.); who the product may be provided to; and how long the license is valid.

In the United States, there are actually two forms of licenses: specific or general. A specific license authorizes one transaction, or a series of transactions. The license applies only to the products and parties identified in the license, and usually has a set period.

A general license, on the other hand, is available to all parties meeting its conditions, and does not require an application. In this way, a general license resembles an exemption. Unlike exemptions, though, a general license may be valid only for a specified period. In addition, the authority administering the sanctions laws may be able to revoke a general license on its own, while changing an exemption may involve a change to the underlying sanctions law itself. For this reason, general licenses may provide somewhat less assurance going forward than supplied by an exemption. The subject of specific and general licenses under U.S. law is addressed in more detail in Chapter 3.

Effectiveness and Unintended Consequences

The purposes of sanctions are to prevent certain types of activities and to persuade (or force) governments and others to change their behavior. One would think that it would be relatively straightforward to measure the effectiveness of sanctions, and that if sanctions were not effective, they would be abandoned. This is not the case. Sanctions are put into place in complex geopolitical situations, and it is often difficult to determine whether they are having a positive effect or not. Empirical research indicates that sanctions are likely to be most effective if the sanctions are focused, and the goal is relatively modest. Arms embargos, for example, tend to be more effective than broader trade restrictions.

Once in place, sanctions have a tendency to remain in place, whether they have proven effective or not. The U.S. embargo against Cuba, for example has been in effect in its current form since 1962, without appreciably changing the behavior of the government in Cuba. On the other hand, international sanctions are credited as being an important factor in South Africa's decision to end apartheid.

Countries do respond to changing situations, however. In contrast to its sanctions against Cuba, the United States ended its sanctions program against Myanmar in 2016 and Sudan in 2017 (although residual sanctions remain in place against each) in response to what were viewed as positive developments in those countries. The

European Union ended most sanctions against Iran following a commitment by that country to limit its nuclear activities.

While the purposes of sanctions are positive, they frequently have unintended consequences. The most obvious of these is to hurt the population of the target country. Even if there are exceptions for agricultural and medical products, it is not unusual for sanctions to make it more difficult for the target country to pay for imports of food and medicine, causing real suffering, especially among the poorest segments of the population. Sanctions can also provide the government of the target country with an excuse for the country's problems, allowing it to whip up resentment and even hatred against the sanctioning country. Sanctions can also, paradoxically, strengthen the economy of the target country in some ways, as it develops domestic industries and supplies to replace imports.

Sanctions can also have a negative effect on the sanctioning country. Companies in the sanctioning country can lose both export markets and sources of supply. Sanctions may drive the target country into a more extreme position, making it difficult to resolve differences diplomatically. Finally, sanctions may create friction between allies if one imposes sanctions and another does not, as has been the case with respect to Iran since the United States ceased to observe the Joint Comprehensive Plan of Action, an agreement the European Union has continued to honor.

The following article from www.sanctionsassociation.org explains unintended consequences of sanctions.

> *The Good, the Bad, and the Ugly: The Unintended Consequences of Sanctions from a Population Perspective*
>
> *August 09, 2019*
> *By: Glenda Juliano from Franklin Templeton Investments*
>
> The U.S. currently maintains economic sanctions against many countries. Frequently criticized and often viewed as a paradox of U.S. foreign policy, economic sanctions are nevertheless quickly becoming the tool of choice for many countries. Sanctions are so popular in fact that many states and municipalities within the U.S. have also begun to implement their own sanctions regimes. In 2000, the U.S. Supreme Court unanimously held in Crosby v. National Foreign Trade Council that a Massachusetts law restricting state transactions with firms doing business in Burma was preempted by federal statute.
>
> Outside of the U.S., it is the policy of the European Union (E.U.) to intervene when necessary, to prevent conflict or to respond to emerging crises by taking the form of restrictive measures or sanctions. Similarly, to the U.S., European sanctions may target governments of third countries, or non-state entities and individuals, such as terrorist groups and terrorists.

Whether a U.S. or E.U., the goal of sanctions is to impose a barrier in hopes of modifying unwanted behavior of a sanctioned party or country. Sanctions are meant to promote international peace and security but may also be applied to prevent conflict and to protect human rights. While the efficacy of sanctions is considered debatable by some, one thing is certain: sanctions have unintended consequences.

Whilst some consequences of imposed sanctions are often perceived as detrimental, not all sanctions have negative consequences.

Sanctions…. A Breeding Ground for Hate?

Former U.S. President, the late Herbert Hoover, once said of sanctions that "they reared incurable hatred".

Though history has shown that in many countries, sanctions have led to increased sympathy for the incumbent government causing a "rally" effect in its population, this is not by any means always the case. It is true that certain beliefs fed by domestic propaganda can create an environment where it is easier to cultivate feelings of hatred, however, there are circumstances when a country has inadvertently benefitted from sanctions.

Let's explore a few examples.

Russia: Bad for Business, Good for Homegrown Farming

For instance, in Russia, direct involvement becomes difficult to handle and many of the smaller international entities are put in positions where they cannot continue to exist in the market, so they leave. This shift allows for big multinational companies to take their place. In some cases, the severity of the sanctions imposed has caused many expat employees to go back to their countries. This, in turn, also creates additional employment opportunities as several countries of the former Soviet Union that are heavily dependent on Russia for employment of their citizens. In the Russian consumer sector, while travel may be limited, those who are able travel to the region can find first class accommodations at a low price due to low occupancy rates. Imported western goods are either eliminated or unaffordable as President Putin imposes restrictions on imports of all western foods and other goods. While the restriction limits or eliminates the flow of supply, this radical change gives an enormous boost to the local farming industry. Russia's agriculture and farming industries are growing rapidly. As an unintended consequence, Russia is transforming under pressure and finding ways to optimize its own economy in the face of new conditions.

Venezuela: A Collective Punishment

Unfortunately, not every country is able to take the same stance.

In Venezuela, the sanctions' regime has created a food deficit which in turn reduces the public's caloric intake and increases disease as well as mortality rates. For countries like Venezuela, sanctions appear to be more of a collective punishment than an attempt to modify behaviors.

In January of 2019, Venezuela was cut off from its primary source of oil consumption – the U.S. In March, Venezuela experienced the first week having zero oil exports, which lasted for another 2 weeks before bouncing back to 1/3rd of their previous year production during this time. Further, sanctions imposed on Venezuela also froze assets and limited access to financial markets consequently exacerbating the humanitarian crisis by limiting access to food and essential imports such as medicine. The economic collapse has also caused problems in the areas of water and sanitation, available electricity, and health care.

Regrettably, Venezuela's President, Nicolas Maduro, has not changed his position and has created an opposition that has clearly demonstrated that sanctions will have a more severe effect on the population by disproportionately harming the poorest and most vulnerable Venezuelans than its government.

Regrettably, Venezuela's President, Nicolas Maduro, has not changed his position and has created an opposition that has clearly demonstrated that sanctions will have a more severe effect on the population by disproportionately harming the poorest and most vulnerable Venezuelans than its government.

Cuba…the failed attempt?

The U.S. originally imposed an arms embargo on Cuba in 1958 during the armed conflict between Fidel Castro's rebel army and President Batista's regime. After Castro gained control of the Cuban government, he began to openly purchase arms from the Soviet Union which led to additional restrictions and reactive shows of force by Castro. Consequently, the U.S. trade embargo of Cuba was initiated in response to a 1960 memo issued by the State Department which proposed a line of action denying money and supplies to Cuba with the purpose of creating hunger, desperation, and the overthrow of the Castro government.

While the U.S. embargo of Cuba certainly caused hunger in the Cuban people, the embargo itself has not affected the Castro government. The U.S. embargo on Cuba consequences are the monetary long-term and short-term outcomes in relation to trade, industry, and the creation of wealth. To date, the government controls all aspects of the economy including the provision of food by rations while the average citizen receives $20 per month. Cuban citizens have found their ways to survive and supplement their income by opening rooms in their homes to host tourist, selling souvenirs and local cuisine to visitors. To the average citizen, this is the way of life and for many generations only life they know. Many humanitarian organizations have criticized the Cuban embargo for its effect on food, clean water, medicine, and other basic needs of the Cuban citizens. Sixty years later, some may even agree that the embargo helps Castro's government remain in control more than it hurts and consider ita failure.

Finding Balance

As sanctions continue to evolve, we see constant change in restrictions and application of regulation to our business practices. Compliance suites have first and foremost, professional responsibility. We are best equipped to conduct business if we educate ourselves and understand the complexity of sanctions. There are many restrictions but there are also areas that allow for certain transactions to be completed. Below are some best practices that can be incorporated and adapted based on business needs:

1. Know Your Customers – maintain detailed information of your customers in a central location accessible to all business areas. The information should be current and frequently maintained.
2. Create and maintain a robust monitoring process.
3. Stay current with regulatory changes and communicate these changes promptly.
4. Seek solutions that integrate system functionalities to make process seamless for the business and the client regardless of your industry.

There is a delicate balance between compliance and service and with the right understanding we can feel confident when allow business processes to flow while managing risk appropriately.

Summary

- Economic sanctions are financial, physical, and other measures taken to prevent certain types of activities or to influence the behavior of countries, groups, or individuals.
- Sanctions may be imposed by a single country, a group of countries, or an international organization.
- The objectives of sanctions include
    - Preventing certain activities, such as terrorism and dealing in narcotics
    - Persuading governments to change their behavior
    - Penalizing (or punishing) the sanctions target
    - Making a symbolic statement

- The history of sanctions dates back at least to classical Athens.
- Since the end of World War I, the use of sanctions has become more common as an alternative to military action.
- Sanctions can be imposed unliterally or multilaterally.
- Sanctions can be broad/comprehensive ("e.g. embargoes") or targeted.
- A sanctions regime is the overall structure of a country's sanctions laws, including
    - Which agency administers and enforces sanctions;
    - The targets of sanctions; and
    - Who must comply with the sanctions.
- A sanctions program refers to the specific sanctions against an individual country or category of persons.
- Sanctions can apply to countries, governments, regions, entities, unofficial groups, individuals, and vessels and aircraft.
- Typical sanctions include
    - Arms embargos
    - Prohibitions on exports
    - Prohibitions on imports
    - Prohibitions on investment
    - Prohibition on financial transactions
    - Prohibitions on making any financial resources available
    - Asset freezes
    - Travel bans.
- Sectoral sanctions are targeted sanctions that apply only to selected sectors of a country's economy.
    - Sectoral sanctions may allow most transactions with the country
- Sanctions typically have certain exceptions for
    - Post and telecommunications
    - Humanitarian donations
    - Family remittances
    - Informational materials.
- A license authorizes a transaction that would otherwise be prohibited by sanctions.
- Sanctions can have unintended consequences, including
    - Causing suffering to the population of the target country
    - Providing an excuse for poor conditions by the government of the target country
    - Loss of export markets and sources of supply in the sanctioning country.

Review Questions

1. What are sanctions?
2. Give three objectives of sanctions.
3. What is the difference between a sanctions regime and a sanctions program?

4. What are the components of a sanctions regime?
5. Who can sanctions apply to?
6. Who must obey a country's sanctions?
7. Give five examples of economic sanctions.
8. Give three examples of exceptions to sanctions.
9. What are some of the unintended consequences of sanctions?

SANCTIONS IMPOSERS AND TARGETS

Association of Certified Sanctions Specialists (ACSS)
7950 NW 53rd Street Suite 337
Miami, FL 33166
Phone: +1 305 433 7187
helpdesk@sanctionsassociation.org
www.sanctionsassociation.org

Introduction

"We don't impose sanctions on Russia for sanctions' sake, rather we impose sanctions to make clear that countries, even if their territorial situation puts them close to Russia, have the right to their own development. Those are the principles of international law."

Angela Merkel (2018)

Economic sanctions are imposed by both countries and international organizations. A sanctions regime is how a polity actually imposes sanctions. The regime includes a number of components:

- The legal sources of sanctions;
- The reasons for imposing sanctions;
- The targets of sanctions;
- The measures being applied, i.e., the types of sanctions;
- Who must comply with sanctions; and
- Compliance and enforcement.

These not surprisingly vary by the individual sanctions regime. One common feature of sanctions regimes world-wide is that they reflect the sanctions imposed by the United Nations, although many go well beyond that. This chapter will discuss the sanctions regime of the United Nations and the major countries who are significant users of economic sanctions, including the European Union, the United States, the United Kingdom, Australia, Canada, and Singapore.

United Nations

From its creation, the United Nations contemplated the use of economic sanctions as an instrument to preserve peace without the need to resort to military force. Since then, the United Nations has declared sanctions in at least 31 cases. The targets have been primarily countries that threaten the peace, although the UN has also sanctioned organizations such as Al Qaeda as well.

Sanctions imposed by the UN do not automatically take effect. Rather, individual countries must implement them through national law or other action. Most UN members do so on an ongoing basis. In addition, many companies have decided to observe UN sanctions, even if not required to do so by national law. For this reason, it is important to understand how and when the UN imposes sanctions, and what the sources for information on UN sanctions are.

Legal Basis: The UN Charter

The ability of the United Nations to impose economic sanctions is found in the UN Charter, the legal document that founded the UN. Article 41 of the Charter provides that:

> The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.

Since 1968, the Security Council has imposed sanctions at least 31 sanctions times. The targets have included, chronologically, Southern Rhodesia, South Africa, Yugoslavia, Haiti, Angola, Liberia, Eritrea/Ethiopia, Rwanda, Sierra Leone, Iran, Côte d'Ivoire, Somalia/Eritrea, , Iraq, the Democratic Republic of Congo, Sudan, Lebanon, North Korea, Iran, Libya, the Taliban, Guinea-Bissau, Central African Republic, Yemen, South Sudan, and Mali. The UN has also imposed sanctions against ISIL (Da'esh), Al-Qaida, and the Taliban The UN currently has 14 programs in effect. Information on these programs can be found on the UN web site.

Did you know?

The **first** UN sanctions program in 1966 was against the illegitimate seizure of power in Southern Rhodesia.

The **oldest** UN sanctions program, still in place today, concerns Somalia (established in 1992).

The **shortest** regime was Eritrea/ Ethiopia, which lasted less than 1 year: 17 May 2000 to 15 May 2001.

The Process

UN sanctions are imposed by the Security Council.

The Security Council can take action to maintain or restore international peace and security under Chapter VII of the United Nations Charter. Sanctions measures, under Article 41, encompass a broad range of enforcement options that do not involve the use of armed force.

The process begins with the Security Council taking up a "situation of concern." Situations that typically give rise to the imposition of sanctions by the UN include:

- massive human rights violations
- illegal smuggling
- activities by extremist groups
- efforts to end civil wars or similar conflicts
- threats to elections
- demobilization of armed groups.

Often just the fact that the Security Council is considering action may be enough to convince the parties involved to change their behavior. If it does not, the Security Council will consider a resolution imposing sanctions and creating a sanctions program. The resolution will specify exactly what measures are to be put into place. Finally, the resolution will establish a committee to oversee the sanctions program in question. Resolutions in the Security Council are subject to veto by one of the permanent members. Because UN sanctions require unanimity on the part of the Security Council, these sanctions, when imposed, represent a broad consensus within the international community that some sort of action is necessary.

The **Committees** carry out the actual work with respect to a sanctions program. Their role is to implement, monitor and provide recommendations to the Council on particular sanctions regimes. A committee may request advice and meet with various Panels of Experts.

Did you know?

Sanctions Committees and Expert Panels

Today, there are 14 ongoing sanctions regimes which focus on supporting political settlement of conflicts, nuclear non-proliferation, and counter-terrorism. Each regime is composed of a sanctions committee chaired by a nonpermanent member of the Security Council. There are ten monitoring groups, teams and panels that support the work of the sanctions committees. Seven are home-based, two are based in New York and one is based in Nairobi. There are a total of 61 experts who report to their respective sanctions committees but are managed by the Security Council Affairs Division (SCAD) of the Department of Political Affairs (DPA). SCAD provides experts with substantive guidance and support, and these monitoring groups, teams and panels cost under $24 million a year.

Source: Feb. 8 2019 Fact Sheets "Subsidiary Organs of the United Nations Security Council"

The committee may also meet with Member States and international organizations. One important function of a committee is to identify exactly who is subject to sanctions. In some cases, the resolution creating a sanctions program may identify individuals or groups that will be subject to the sanctions, but in many cases, it is the responsible committee that does so.

Action by the Security Council is also needed to remove sanctions. The Security Council will lift sanctions when and if the situation underlying the imposition of sanctions has been resolved.

UN sanctions do not automatically go into effect in individual countries, and the UN has no independent mechanism for enforcing sanctions. Rather, sanctions must be implemented by the individual members. Most UN members have a process where UN sanctions, including new designations, are incorporated into national law. This process typically requires the enactment of legislation or regulation that adopts the UN sanctions. In addition, many companies have the policy of declining to do business with individuals or entities that are subject to UN sanctions, even if their country has not imposed those sanctions.

Designation

The United Nations can and does impose sanctions against entire countries, such as is currently the case with North Korea. More commonly, though, sanctions are imposed against individuals and entities. Even though the United Nations will impose sanctions against a country, those sanctions usually take the form of measures targeted at named individuals or entities rather than the government or the country as a whole (North Korea again being a notable exception). The types of actions that can lead to designation by the United Nations include:

- threats to peace, security or stability;
- violations of human rights and international humanitarian law;
- obstructing humanitarian aid;
- recruiting or using children in armed conflicts;
- targeting civilians including killing and maiming, sexual and gender-based violence, attacks on schools and hospitals, and abduction and forced displacement;
- engaging in illegal trade in natural resources;
- violations of arms embargoes;
- acts or financing of terrorism;
- engaging in or providing support for nuclear, weapons of mass destruction and/ or ballistic missile programs and policies.

Once a person or entity is designated, it is placed on the UN's Consolidated List, which can be found at:

https://www.un.org/securitycouncil/content/un-sc-consolidated-list#composition%20list.

Types of Sanctions

In the past, the UN has imposed very broad sanctions, including complete trade embargos. Since 2004, it has relied on more focused sanctions. Current sanctions methods include:

- travel bans;
- asset freezes;
- arms embargoes;

- bans on trade in certain commodities, such as diamonds, timber, petroleum, and charcoal;
- bans on exports of certain items to the country;
- bans on imports of selected items from the country;
- restrictions on exports to the country of goods and technology related to nuclear, ballistic missiles and other weapons of mass destruction; and
- bans on the export of certain luxury goods.

These measures can apply to individuals, entities, or entire countries. For example, the arms embargo against Somalia applies to the entire country except for arms shipments to the Federal Government of Somalia, which are nonetheless subject to strict controls.

Current Sanctions Programs

The United Nations currently has 14 sanctions programs in place. Of these, 12 apply to countries, while two are directed against entities. As noted above, sanctions programs against countries may in fact target specific individuals and entities rather than the entire country. The following are the programs in effect as of August 2019. The number refers to the number of the resolution in the Security Council instituting the sanctions.

1. Somalia (Resolution 751
2. ISIL (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities (Resolutions 1267, 1989 and 2253)
3. Iraq (Resolution 1518)
4. Democratic Republic of the Congo (Resolution 1533)
5. Sudan (Resolution 1591)
6. Lebanon (Resolution 1636)
7. North Korea (Resolution 1718)
8. Libya (Resolution 1970)
9. Taliban (Resolution 1988)
10. Guinea-Bissau (Resolution 2048)
11. Central African Republic (Resolution 2127)
12. Yemen (2140)
13. South Sudan (Resolution 2206)
14. Mali (Resolution 2374)

De-listing Mechanisms

The United Nations is very aware of the potential impact of inclusion on its sanctions list. As a consequence, it has two separate procedures by which individuals and entities can seek to be removed from the list.

First, there is a specific "Focal Point for De-Listing." An individual or entity (except for those on the ISIL and Al-Qaida list) can file an application with the Focal Point for De-listing seeking removal from a sanctions list. The Focal Point also receives requests for exemptions from travel bans and assets freezes exemption requests from individuals and entities on the ISIL (Da'esh) and Al-Qaida and the Taliban Sanctions lists. While the Focal Point receives and processes such requests, the actual decision whether to de-list rests with the relevant sanctions committee.

Requests for removal from the ISIL and Al-Qaida lists are handled by the Office of the Ombudsman.

European Union

The European Union is one of the major users of economic sanctions. The EU system is unusual in that, although sanctions are promulgated by and for the EU as a whole, they must be implemented and enforced by the individual members. In addition, EU members may impose sanctions that go beyond those of the EU itself.

The EU refers to sanctions as both "sanctions" and as "restrictive measures." They are considered to be preventive, non-punitive, instruments that allow the EU to respond swiftly to political challenges and developments. The reasons the EU imposes sanctions include:

- Safeguarding values, interests and security
- Preserving peace
- Consolidating and supporting democracy, the rule of law, human rights, and principles of international law
- Preventing conflicts and strengthening international security

EU's Common Security and Foreign Policy (CFSP)

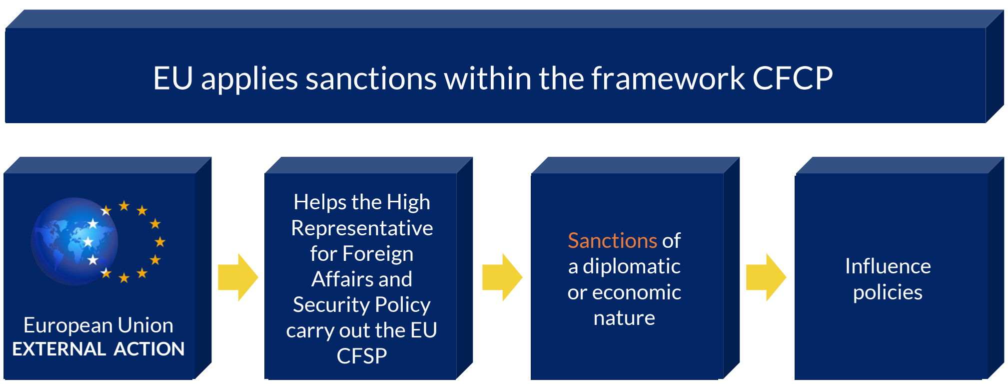
The EU is made up of 28 members states and seven different decision making bodies, most of which were established during the inception of the EU in 1958. This includes two legislative bodies called the Council of the European Union (the Council) and the European Parliament. Sanctions have become an increasingly important tool of the EU's Common Security and Foreign Policy (CFSP). According to Articles 29 and 31 of the Treaty of the European Union (TEU), the Council must adopt CFSP decisions involving sanctions on a unanimous basis among Member States.

Legal Basis

The EU applies Sanctions within the framework of the Common Foreign Security Policy. This is the agreed foreign policy by the members of the EU. Sanctions are one element of this foreign policy. The legal basis for the imposition of sanctions by the EU is Article 215 of the Treaty on the Functioning of the European Union, which states that

1. Where a decision, adopted in accordance with Chapter 2 of Title V of the Treaty on European Union, provides for the interruption or reduction, in part or completely, of economic and financial relations with one or more third countries, the Council, acting by a qualified majority on a joint proposal from the High Representative of the Union for Foreign Affairs and Security Policy and the Commission, shall adopt the necessary measures. It shall inform the European Parliament thereof.
2. Where a decision adopted in accordance with Chapter 2 of Title V of the Treaty on European Union so provides, the Council may adopt restrictive measures under the procedure referred to in paragraph 1 against natural or legal persons and groups or non-State entities.
3. The acts referred to in this Article shall include necessary provisions on legal safeguards.

Common Foreign and Security Policy (CFSP)



Source: ACSS EU Restrictive Measures Essentials Course

The EU has set out its fundamental sanctions policies in the Basic Principles on the Use of Restrictive Measures (Sanctions), which was issued by the EU Council in 2004. A link to the text of this document is included in the reference materials. The first principle is that We are committed to the effective use of sanctions as an important way to maintain and restore international peace and security in accordance with the principles of the UN Charter and of our common foreign and security policy. In this context, the Council will work continuously to support the UN and fulfil our obligations under the UN Charter… We will ensure full, effective and timely implementation by the European Union of measures agreed by the UN Security Council.

While UN sanctions are not self-executing, this principle means that the EU will apply all UN sanctions. In addition, the EU will apply autonomous sanctions to meet various goals, including

- to fight terrorism and the proliferation of weapons of mass destruction
- a restrictive measure to uphold respect for human rights, democracy, the rule of law and good governance.

This occurs in the context of the Common Foreign and Security Policy. Sanctions are only one element in an integrated policy that also uses dialog, incentives, and conditionality to achieve these goals. At the same time, sanctions should be tailored in a way that maximizes the effects on the target, while minimizing adverse effects on others. For this reason, EU sanctions tend to be targeted towards specific individuals and entities, rather than whole regions or countries.

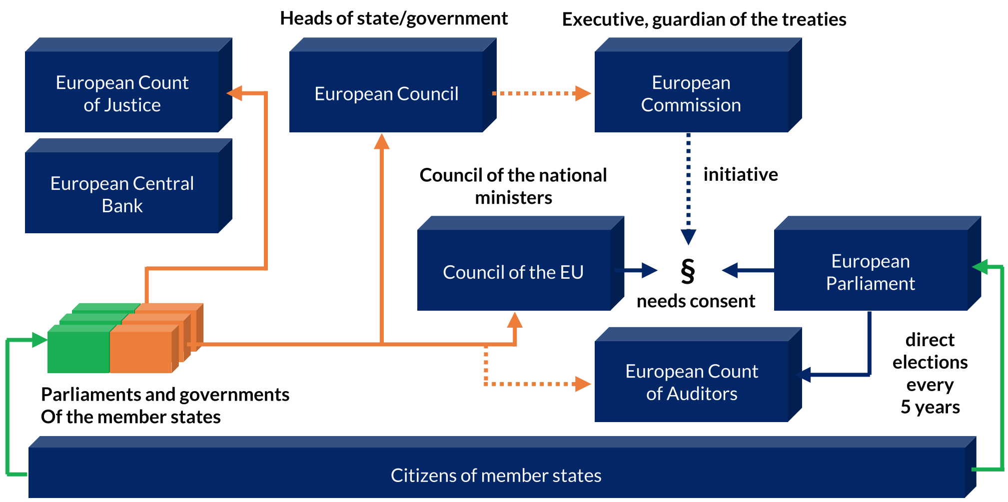
The EU publishes and periodically updates both its “guidelines” and “best practices” in connection with restrictive measures. The current versions of these documents, Sanctions Guidelines – update and Restrictive measures (Sanctions) - Update of the EU Best Practices for the effective implementation of restrictive measures, were published in 2018, and links are contained in the reference materials annex. These provide further detail on the goals, legal requirements, and internal organization of restrictive measures.

The Process

As you can imagine, the structure of the European Union is rather complex. First of all it has member states, each with its own legislative, executive and judicial system. In the image below, you can see the main seven EU bodies: European Court of Justice, European Central Bank, European Council – this is a body with heads of the states of the member states, then Council of the EU - this is the council of national ministers, European Commission, the so-called executive branch, and finally the European Parliament and European Court of Auditors.

Article 215 provides the general framework for the imposition of sanctions by the EU. As the article requires, sanctions take the form of a measure passed by the EU Council. The measures may be directed against countries or against “natural or legal persons and groups or non-State entities.” Action by the Council begins when it receives a joint proposal from the High Representative of the Union for Foreign Affairs and the EU Commission identifying a problem and recommending the imposition of restrictive measures. After considering the proposal, the Council will decide, by a qualified majority vote (i.e., votes representing at least 65% of the EU population), whether to impose restrictive measures.

Overview of main EU bodies



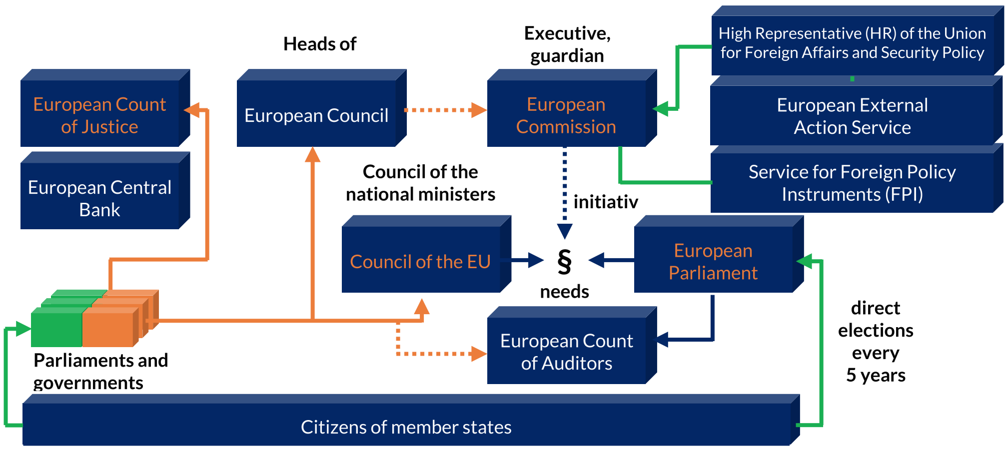
The restrictive measures initially take the form of a Council decision. The decision will typically contain several elements, including

- The target of the restrictive measures (the country, individuals, or entities, which are usually identified in an Appendix to the decision)
- The reasons the measures are being imposed
- A direction that the Member States "shall take the necessary measures" to implement and enforce the restrictive measures
- A detailed description of the restrictive measures
- Any exceptions or exemptions to the measures that may apply
- The procedure for imposing restrictive measures on additional persons or entities

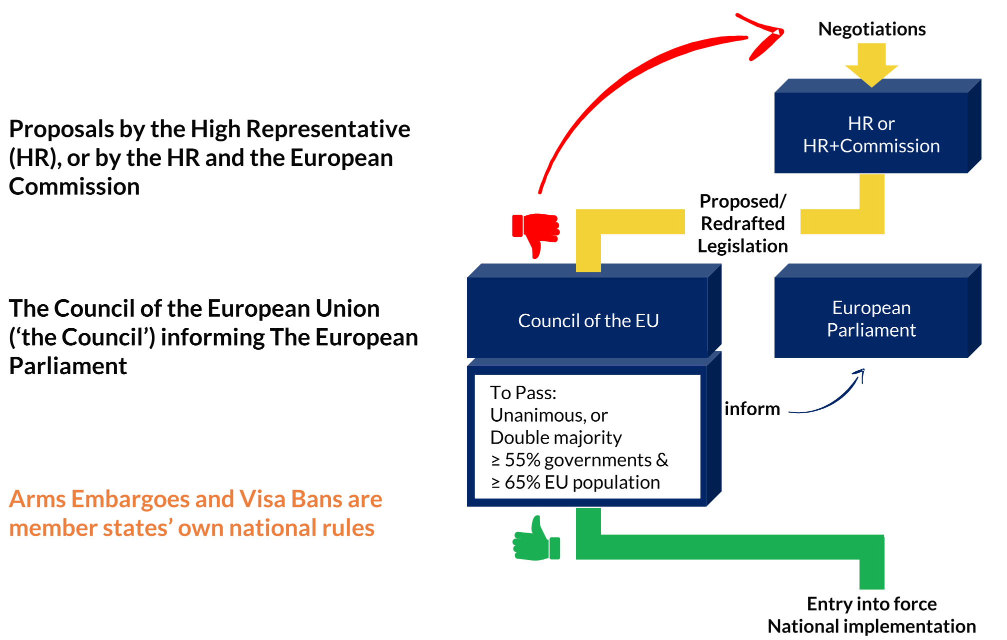
While the Council will inform the EU Parliament of the decision, no approval by the Parliament is required, so that the decision takes effect once it is issued by the Council.

Sanctions are initially imposed by a Council decision that applies measures to the country (or, more commonly, individuals and entities within the country) for the first time. The Council may subsequently issue additional decisions modifying the previous measures by, for example, adding new persons to the list. Decisions that broaden or restrict the scope of sanctions are simply called "Decisions," while decisions adding or removing individuals and entities from the applicable sanctions list are described as "Implementing Decisions." Decisions to extend measures are also common.

Overview of EU bodies that get involved



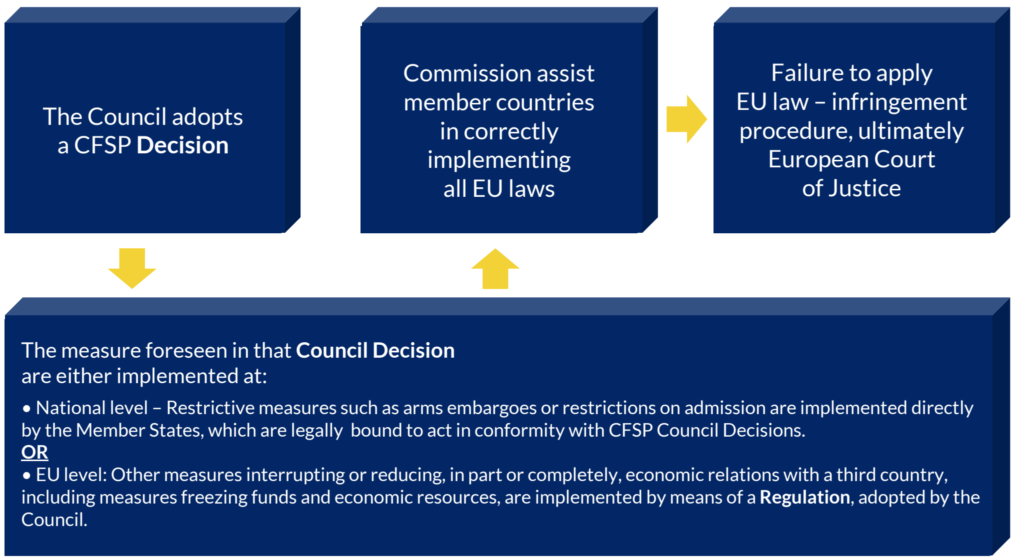
How are EU Restrictive Measures adopted?



The Council may also issue regulations under the decision, providing more detail, including definitions that apply to the decision such as, for example, the definition of “economic resources.” A Council regulation is required when the restrictive measures include an asset freeze or other financial or economic sanctions, where precision delineating exactly what is and is not allowed is necessary.

Restrictive measures go into force when they are published in the EU Journal. Although sanctions are adopted at the EU level, the EU does not have the ability to enforce sanctions. Rather, they are enforced by national regulators at the national level. Additional action may also be necessary at the national level to implement travel bans and arms embargoes in particular. Trade and financial sanctions, on the other hand, have automatic EU-wide effect, although again enforcement is by the individual Member States. Finally, Member States may impose sanctions beyond those imposed by the EU. This typically takes the form of the designation of additional individuals or entities under existing Council decisions, but could include broader measures as well. A more detailed discussion of the sanctions enforcement regimes of the EU Member States appears below.

Implementation at the Member States



Types of Restrictive Measure

Most EU restricted measures today are “targeted”. This simply means that they purport to channel harm toward specific public figures and entities, while maintaining the economic status quo of the country being sanctioned. Targeted sanctions are thus implemented in such a way that they only affect certain individuals, organizations, elites or economic sectors rather than the country’s entire economy. This notably excludes comprehensive trade embargoes (such as the US embargo of Cuba) owing to their indiscriminate effects. In some cases, though, the EU will impose restrictive measures on an entire region or country, as is true with respect to Crimea, North Korea, and Syria, for example.

The EU periodically publishes a compendium of all the restrictive measures in force. EU restrictive measures can be divided into four main categories: arms embargoes, travel bans, economic and trade measures, and financial measures.

Arms embargoes prohibit the sale weapons and related services to restricted individuals, groups, or states. The language of Council Decision 2013/798/CFSP, which imposed restrictive measures on the Central African Republic, is typical:

> The sale, supply, transfer or export of arms and related materiel of all types, including weapons and ammunition, military vehicles and equipment, paramilitary equipment, and spare parts for the aforementioned to the Central African Republic ('CAR') by nationals of Member States or from the territories of Member States or using their flag vessels or aircraft shall be prohibited whether originating or not in their territories.

The definition of "arms" is fairly broad, and include weapons and ammunition, military vehicles and equipment, paramilitary equipment, and spare parts. In addition to a ban on arms sales, arms embargoes also include a prohibition on providing technical assistance and brokering services related to arms sales; the provision, manufacture, maintenance, or use of arms and related materials; and financing of such transactions. Taking steps to circumvent an arms embargo is also prohibited. On the other hand, the restrictive measures may include specific exemptions; the arms embargo against the Central African Republic, for example, exempts the supply of arms to UN personnel in the CAR from the general prohibition.

In cases where restrictive measures are imposed in response to concerns about the lack of democracy and respect for human rights and the rule of law, the EU may also impose a ban on the export of equipment which might be used for internal repression. Similarly, the EU may ban the export of dual-use goods, services, or technology when they are intended for military use. Conversely, the EU may also prohibit imports of arms and military equipment from sanctioned countries, as with North Korea.

Travel bans consist of restrictions or prohibitions on travel by designated individuals to the EU. The standard language used is "Member States shall take the necessary measures to prevent the entry into, or transit through, their territories of individuals referred to in" the relevant article of the decision. Members are not required to deny entry to their own nationals, though. Because the Member States continue to control their own immigration, action by each member is required to implement travel bans.

Somewhat similar to a travel ban is requirement to close offices of sanctioned parties, as well as a prohibition on the establishment of new branches or offices.

Economic measures may include a variety of measures, including prohibitions or restrictions on imports and exports of goods and services to countries, entities, or individuals. These are primarily goods and services that could be used by targeted actors to pursue a restricted objective. They may also include restrictions on investment in particular regions or countries. Economic measures may also limit trade and transportation directly.

Trade in goods and services: Economic measures affecting trade in goods, services, and technology can take a variety of forms. The most extensive measure is an embargo, which prohibits both imports and exports of designated goods and services from the target country. The following excerpt from Article 12 of Council Decision 2013/255/CFSP, which imposed restrictive measures on Syria, is an example of the type of language used to impose an embargo:

> The direct or indirect sale, purchase, transportation or brokering of gold and precious metals, as well as of diamonds to, from or for the Government of Syria, its public bodies, corporations and agencies, the Central Bank of Syria, as well as to, from or for persons and entities acting on their behalf or at their direction, or entities owned or controlled by them, shall be prohibited.

Narrower but still broad measures may include a total ban on imports from the region or country, as is true with Crimea, where the relevant Council Decision states simply “The import into the Union of goods originating in Crimea or Sevastopol shall be prohibited.” More commonly, restrictive measures may prohibit the import of select goods, typically those the target country sells in international markets, such as metals and petroleum products.

Conversely, economic measures may include restrictions on exports of goods and services. Besides military and dual-use goods, examples of goods subject to import and/or export bans include gold, precious metals, and diamonds; petroleum products; luxury goods; aviation fuel; and telecommunications. In some circumstances, exports may be allowed, but only with prior authorization. Trade restrictions normally prohibit financing, brokering, and insuring trade in the goods as well, as well as services associated with them, such as telecommunications services.

Finally, trade measures may restrict exports of all goods, services, and technology to a specific sector or industry in the target country. An example is the prohibition on exports to certain energy projects in Russia, which is discussed below.

Investment: A less common type of economic sanction is a prohibition or restriction on investment. These restrictions normally target specific sectors, such as real estate, energy, or nuclear power. A wider prohibition is that on investment by EU nationals in any entity in Crimea. Sanctions may also prohibit investment by nationals of the target country in designated sectors of the EU economy, such as nuclear power or arms. As with trade in goods and services, restrictions on investment may apply to the provision of investment services as well.

Other trade-related measures: The EU may also impose direct restrictions on trade and transportation. This can include prohibiting the use of EU-registered aircraft or vessels for trade with the country; transit through or export from the EU of goods or services that are not of EU origin; and denial of the right of vessels or aircraft from a target country to use EU ports or airports. EU nationals may also be prohibited from leasing vessels or aircraft to nationals of the target country.

Prior information on, and inspection of, cargoes going to or from the target country may be required.

Financial measures prohibit financial transactions with the target, and may even require the freezing of assets belonging to sanctioned individuals or entities. In such cases, the Council decision will require that "{a}ll funds and economic resources belonging to, or owned, held or controlled by" a sanctioned party must be frozen. The definitions of both "funds" and "economic resources are broad. The definition of "funds" encompasses

- cash, checks, claims on money, drafts, money orders and other payment instruments;
- deposits with financial institutions or other entities, balances on accounts, debts and debt obligations;
- publicly- and privately-traded securities and debt instruments, including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures and derivatives contracts;
- interest, dividends or other income on or value accruing from or generated by assets;
- credit, right of set-off, guarantees, performance bonds or other financial commitments;
- letters of credit, bills of lading, bills of sale; and
- documents evidencing an interest in funds or financial resources;

"Economic resources" can include practically anything of value, including "'assets of every kind, whether tangible or intangible, movable or immovable, which are not funds but may be used to obtain funds, goods or services."

The freezing of funds requires

> Preventing any move, transfer, alteration, use of, access to, or dealing with funds in any way that would result in any change in their volume, amount, location, ownership, possession, character, destination or other change that would enable the funds to be used, including portfolio management."

Similarly, freezing economic resources means "preventing their use to obtain funds, goods or services in any way, including, but not limited to, by selling, hiring or mortgaging them." Frozen funds must be placed in a blocked account, and not released without permission of the relevant national authority. Other, non-financial property can also be frozen, meaning that it may not be bought, sold, transferred, or otherwise disposed of without permission. There are specific circumstances under which a sanctioned party may nonetheless have access to frozen funds, such as to pay for necessary living expenses. These exceptions are set forth in the decision as well.

Financial sanctions may also prohibit EU persons from making any "economic resources" available to the sanctioned party. Such a restriction prohibits basically all transactions with a sanctioned person.

Financial sanctions can target some types of financial transactions specifically. At their widest, sanctions may prohibit all transfers of funds to or from the target country. Sanctions may also limit other types of banking transactions, the provision of insurance and reinsurance, and trade in bonds and equity, as well as transferable securities and money market instruments. An even more targeted type of financial sanctions are so-called "sectoral sanctions," which prohibit EU nationals from buying, selling, or trading in transferable securities, money market instruments, or equity of certain Russian banks and energy companies. In such cases, only the designated types of transactions are banned; all other transactions are legal. In the case of designated Russian banks, for example, this means that EU banks can continue to process payments and other funds transfers to and from them.

Licenses

The competent national authorities can issue licenses authorizing transactions that restrictive measures would otherwise prohibit. In cases of asset freezes, the authority may allow the release of funds for certain basic purposes, including

1. Meeting basic needs, including food, housing, medicine and medical care, insurance premiums, and utilities;
2. The payment of legal fees; and
3. The payment of certain claims following a decision by a judicial or arbitral authority.

National authorities may also authorize other prohibited transactions, depending upon national law.

Targets of Sanctions

As noted above, the EU prefers to target sanctions as narrowly as possible to maximize their impact and to avoid negative consequences for "innocent bystanders." Accordingly, most EU restrictive measures are directed against named individuals and entities. Entities may include companies, as well as organizations like Al Qaida. The EU may even direct sanctions against vessels, by "freezing" them, i.e., prohibiting any transactions involving them.

The EU maintains a full list of the individuals and entities subject to restrictive measures, the "Consolidated list of persons, groups and entities subject to EU financial sanctions," which can be found at http://data.europa.eu/euodp/en/data/dataset/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions. For each person or entity, the list provides the person or entity's name; any aliases used; and a description of who or what they are and why they are being sanctioned. Names are always given in the Latin alphabet; names may also be provided in the Cyrillic alphabet, if relevant. For natural persons, the list also shows the birth date and place of birth, if available.

Individual Member States maintain their own sanctions lists, which may include additional names. In addition, Member States may request that particular persons or entities be added to the EU list. This proposal is typically submitted to, and initially reviewed by, the EU Presidency. Third states may also request designation. The request for designation must be supported by credible evidence supporting the request. The request, with the supporting information, then circulates through the Member States for review. In the case of terrorism designations, for example, the proposal is submitted to the CP 931 Working Party. After reviewing the information, the Working Party makes its recommendation to the Permanent Representatives Committee ("COREPR"). If the COREPR endorses the recommendation, it is forwarded to the EU Council for final approval.

Persons and entities on the sanctions list can seek to be delisted by applying to the appropriate committee. They can also seek legal redress through national courts or the EU Court of First Instance. While courts can review whether the legal criteria for listing, such as support by credible information, were satisfied, they cannot second-guess the political decision to add a person to the sanctions list.

Not all entities subject to sanctions are necessarily included on the EU sanctions list, though. Entities in which a sanctioned person or entity has an ownership interest of more than 50 percent are also subject to restrictive measures, even if they are not designated separately. The same applies to entities that are controlled by sanctioned persons. The EU's Update of the EU Best Practices for the effective implementation of restrictive measures lists the following factors as evidence that a designated person controls an entity includes:

- having the right or exercising the power to appoint or remove a majority of the members of the entity's administrative, management or supervisory body;
- having appointed solely as a result of the exercise of one's voting rights a majority of the members of the administrative, management or supervisory bodies of the entity in the present and previous financial years;
- controlling alone, pursuant to shareholder agreement, a majority of shareholders' or members' voting rights;
- having a legal right to exercise a dominant influence over the entity;
- having the right to use all or part of the assets of a legal person or entity;
- managing the business of an entity on a unified basis, while publishing consolidated accounts;
- sharing jointly and severally the financial liabilities of the entity, or guaranteeing them.

The presence of any of these factors can establish control. If the relevant legal authority (typically the national enforcement agency) finds control exists, the entity is subject to the same restrictive measures as the individual or entity controlling it.

In some cases, restrictive measures are targeted at entire countries or regions. At present, the countries to which country-wide sanctions (other than an arms embargo) apply include Crimea, Iran, North Korea, and Syria.

Who Must Comply with EU Sanctions

EU sanctions apply:

- With respect to any activity within the territory of the Union; on board any aircraft or any vessel under the jurisdiction of a Member State;
- to any person inside or outside the territory of the Union who is a national of a Member State;
- to any legal person, entity or body, inside or outside the territory of the Union, which is incorporated or constituted under the law of a Member State; and
- to any legal person, entity or body in respect of any business done in whole or in part within the Union.

EU nationals include citizens of the Member States, as well as companies and other entities organized under the laws of a Member State. Such persons, whether natural or legal, must comply with all EU sanctions regardless of where they are located. Foreign subsidiaries of EU companies – i.e., entities organized under the laws of a country that is not a Member State -- may not be required to comply with EU sanctions, and can do things prohibited for their EU parents or subsidiaries. Determining what is and is not allowable under such circumstances is complicated, and may depend upon the form of legal organization and the extent to which EU persons, including the EU parent, are involved in either general decisions or specific transactions. Branches abroad of EU companies, on the other hand, are considered to be EU nationals.

Persons of any nationality who are physically present in the EU must also comply with EU sanctions.

EU Sanctions Programs

The EU currently has in place sanctions programs directed at 34 countries, although in most cases the restrictive measures are directed at individuals and entities rather than being country-wide. Sanctions are also in place with respect to various terrorist groups. These are the EU programs now in force, with a brief description of the applicable sanctions.

1. Afghanistan: EU sanctions against Afghanistan are directed primarily at the Taliban and persons associated with it.
2. Belarus
3. Bosnia and Herzegovina
4. Burundi
5. Central African Republic
6. China
7. Democratic Republic of Congo
8. Egypt
9. Eritrea
10. Guinea
11. Guinea-Bissau
12. Haiti
13. Iran
14. Iraq
15. Lebanon
16. Libya
17. Moldova (Transnistrian region)
18. Myanmar
19. North Korea
20. Russian Federation
21. Somalia
22. South Sudan
23. Sudan
24. Syria
25. Ukraine (Crimea and Sevastopol)
26. Yugoslavia
27. Zimbabwe

Practically all of these programs include arms embargos, travel bans, and asset freezes. The sanctions against North Korea and Syria, and to a lesser extent Iran, are more extensive, and include economic/trade and financial sanctions as well.

The sanctions against Russia are more limited, but include sectoral sanctions against certain Russian banks, as well as bans on exports of goods, services, and technology for certain oil projects in Russia. Here is an example of a Council Regulation that covers this topic.

“COUNCIL REGULATION (EU) No 960/2014

of 8 September 2014

amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 215 thereof,

Having regard to Council Decision 2014/659/CFSP of 8 September 2014 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine (1),

Having regard to the joint proposal of the High Representative of the Union for Foreign Affairs and Security Policy and of the European Commission,

Whereas:

(1) Council Regulation (EU) No 833/2014 (2) gives effect to certain measures provided for in Council Decision 2014/512/CFSP (3). Those measures comprise restrictions on exports of dual-use goods and technology, restrictions on the provision of related services and on certain services related to the supply of arms and military equipment, restrictions on the sale, supply, transfer or export, directly or indirectly, of certain technologies for the oil industry in Russia in the form of a prior authorisation requirement, and restrictions on access to the capital market for certain financial institutions.

(2) The Heads of State or Government of the European Union called for preparatory work on further targeted measures to be undertaken so that further steps could be taken without delay.

(3) In view of the gravity of the situation, the Council considers it appropriate to take further restrictive measures in response to Russia's actions destabilising the situation in Ukraine.

(4) In this context, it is appropriate to apply additional restrictions on exports of dual-use goods and technology, as laid down in Council Regulation (EC) No 428/2009 (4).

(5) In addition, the provision of services for deep water oil exploration and production, arctic oil exploration and production or shale oil projects should be prohibited.

(6) In order to put pressure on the Russian Government, it is also appropriate to apply further restrictions on access to the capital market for certain financial institutions, excluding Russia-based institutions with international status established by intergovernmental agreements with Russia as one of the shareholders; restrictions on legal persons, entities or bodies established in Russia in the defence sector, with the exception of those mainly active in the space and nuclear energy industry; and restrictions on legal persons, entities or bodies established in Russia whose main activities relate to the sale or transportation of crude oil or petroleum products. Financial services other than those referred to in Article 5 of Regulation (EU) No 833/2014, such as deposit services, payment services, insurance services, loans from the

institutions referred to in Article 5(1) and (2) of that Regulation and derivatives used for hedging purposes in the energy market are not covered by these restrictions. Loans are only to be considered new loans if they are drawn after 12 September 2014.

(7) These measures fall within the scope of the Treaty and, therefore, in particular with a view to ensuring its uniform application in all Member States, regulatory action at the level of the Union is necessary.

(8) In order to ensure that the measures provided for in this Regulation are effective, it should enter into force immediately,

HAS ADOPTED THIS REGULATION: (...)"

The regulation can be found here:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0960

EU Blocking Statute

The European Union tends to cooperate closely with the United States, as well as with its other allies, in imposing sanctions. In certain cases, though, U.S. law purports to prohibit EU subsidiaries of U.S. firms from engaging in certain transactions, such as doing business with Cuba and, in some instances Iran, that are completely legal under EU law. U.S. sanctions also threaten to penalize EU firms that do business with certain U.S. sanctions targets, including persons and entities in Iran and Russia. In response, the EU has enacted a blocking regulation, Council Regulation (EC) No 2271/96 that prohibits EU companies from complying with sanctions that are not imposed by the European Union. The regulation was updated in 2018 in response to U.S. secondary sanctions against Iran.

Although the extension of U.S. sanctions to prohibit actions by EU companies is politically controversial, the EU has never actually penalized any company for complying with U.S. sanctions. This may reflect in part the fact that the United States has not yet punished any EU entities for "violating" U.S. sanctions. Some governments, such as that of Netherlands, have stated that, despite the blocking regulation, companies can decide where they will do business.

Compliance

The EU does not have specific requirements for systems for complying with EU sanctions. Nor do the individual members. The EU has provided draft guidance on best practices for internal compliance programs ("ICPs") for dual-use regimes (contained in the Appendix or here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.205.01.0015.01.ENG&toc=OJ:L:2019:205:TOC). While this guidance is technically directed towards export controls rather than sanctions, the guidance references sanctions in several places, and the same principles apply. The draft guidance accordingly provides a solid framework for the creation of sanctions compliance programs by EU entities.

The guidance states that an internal compliance system "needs to be tailored to the size, the structure and scope of the business, and especially, to the company's specific business activity." The starting point for this process is a risk assessment to identify the entity's sanctions risks. Once those risks have been identified, it is possible to design and create a system that mitigates those risks. The core elements of an effective compliance system, and the principles underlying those elements, include:

1. **Top-level management commitment to compliance:** "Effective ICPs reflect a top-down process whereby the company's top-level management gives significance, legitimacy, and organizational, human and technical resources for the corporate compliance commitments and compliance culture."
2. **Organization structure, responsibilities and resources commensurate to the entity's risk profile**: "Sufficient organizational, human and technical resources are essential for effectively developing and implementing compliance procedures. Without a clear organization structure and well-defined responsibilities, an ICP risks suffering from lack of oversight and undefined roles. Having a strong structure helps organisations work out problems when they arise and prevent unauthorized transactions from occurring."
3. **Training and awareness raising:** "Training and awareness raising … is essential for staff to duly perform their tasks and take compliance duties seriously.
4. **Transaction screening process and procedures:** "In terms of operational implementation, transaction screening is the most critical element of an ICP. This element contains the company's internal measures to ensure that no transaction is made without the required license or against any relevant trade restriction or prohibition. The transaction screening procedures collect and analyze relevant information concerning item classification, transaction risk assessment, license determination and application, and post-licensing. Transaction screening measures also allow the company to develop and maintain a certain standard of care for handling suspicious enquiries or orders."
5. **Performance review, audits, reporting and corrective actions:** "An ICP is not a static set of measures and therefore must be reviewed, tested and revised if proven necessary for safeguarding compliance. Performance reviews and audits verify whether the ICP is implemented to operational satisfaction and is consistent with the applicable national and EU export control requirements.

A well-functioning ICP has clear reporting procedures about the notification and escalation actions of employees when a suspected or known incident of non-compliance has occurred. As part of a sound compliance culture, employees must feel confident and reassured when they raise questions or report concerns about compliance in good faith. Performance reviews, audits and reporting procedures are designed to detect inconsistencies to clarify and revise routines if they (risk to) result in non-compliance."

6. **Recordkeeping and documentation:** "Proportionate, accurate and traceable recordkeeping … is essential for your company's compliance efforts. A comprehensive recordkeeping system will help your company with conducting performance reviews and audits, complying with national documentation retention requirements and it will facilitate cooperation with competent authorities …."

The draft guidance provides step-by-step recommendations for each element in the internal compliance program.

Enforcement

Although the EU has deployed sanctions extensively, it has relatively little experience in enforcing them. As noted above, it is left to the Member States to ensure that their nationals comply with EU sanctions. The enforcing agencies and the penalties for violation are established by Member State laws and regulations, and vary across the EU.

Member State Sanctions Regimes

It is left to the Member States to actually enforce EU restrictive measures. Member States may also impose their own restrictive measures, primarily through the designation of additional individuals or entities, so long as they are consistent with broader EU regulation. Each Member State therefore has its own sanctions regime. Some of the major ones are discussed below.

United Kingdom

As of the writing of this guide, the United Kingdom was still in the EU, and was still subject to EU sanctions laws. Now that the U.K. has formally triggered the process of exiting the EU, the future effect of EU laws involving sanctions is unknown. In the meantime, the UK has implemented probably the most independent and far-reaching system of sanctions enforcement in the EU.

As of March 2016, the UK has created the new Office of Financial Sanctions implementation (OFSI) (replacing the HM Treasury's Asset Freezing Unit), which is responsible for the implementation and administration of international financial sanctions in the UK. The Department for Business, Innovation & Skills (BIS) is responsible for trade sanctions. The OFSI, a part of Her Majesty (HM)'s Treasury Department of the U.K. government, is the authority for the implementation of financial sanctions in the U.K.

The OFSI keeps a list of 'designated persons', or 'targets'. A designated person means anyone, whether an individual, company or country, that is subject to financial sanctions and appears on the OFSI's "consolidated list of targets".

To fall within the OFSI's enforcement of sanctions, there has to be a U.K. connection to the breach, or so-called "U.K. nexus". As the breach does not have to occur within U.K. borders, such a nexus is not a difficult one to create. The following situations are just some examples of what can create a U.K. nexus:

- a U.K. company working overseas;
- an international transaction clearing or transiting through the U.K.;
- an action by a local subsidiary of a U.K. parent company; or
- purchase/sale of financial products or insurance on U.K. markets, even if held or used overseas.

This means that a UK company with only one overseas subsidiary or a company clearing just one international transaction through the U.K may be caught by U.K. sanctions requirements and could be liable for violations committed against U.K. financial sanctions. The previous principle that European sanctions do not extend to foreign subsidiaries or non-EU persons is no longer true in this respect.

The following article on www.sanctionsassociation.org explains the effect of Brexit on UK sanctions regime.

The 'Brexit' Effect: What the UK's Departure from the EU Could Mean for the Global Sanctions Landscape

December 9, 2019
By: John McKendrick QC and Alex Haines from Outer Temple Chambers

Over three years ago, in the June 23 Referendum, the UK voted to leave the European Union (EU). This departure from the EU, also known as 'Brexit', has put the world on stand-by, waiting to see what terms the UK and Europe will decide for their future divorce. One of these terms will be how to treat sanctions policy once the UK leaves.

The European sanctions landscape is already vastly complex, partly due to the different – and often opposed – political agendas as well as the ever-changing convergence between sanctions law, international law, and the domestic law of sovereign EU states. The numerous permutations – at a time where: (i) the UK is due to depart the EU but has not yet done so; (ii) the US has withdrawn from the Joint Comprehensive Plan of Action (or Iran nuclear deal); and (iii) the EU announced the reactivation of the Blocking Regulation – compound the uncertainty and make it increasingly difficult for businesses to accurately follow and understand the provisions that affect them.

Now, as the January 31 deadline for Brexit looms, companies and compliance suites are becoming more and more eager to learn if the split will cause a rift between EU and UK sanctions policy or if it will, in fact, have any significant impact on the UK sanctions landscape at all.

UK Sanctions on the World-Stage

As a global hub for finance and banking, the UK has always played a powerful role in European sanctions policy and implementation.

According to Erica Moret and Fabrice Pothier in their book "Sanctions after Brexit" (Survival, vol. 60 no.2, April-May 2018, pp. 179-180): "As a leading political, economic and soft-power actor, and home to one of the world's premier financial centres (the City of London), the UK has traditionally played a central role in shaping EU sanctions, contributing to their design and implementation, and participating in intelligence-sharing and consensus-building among member states. It is unlikely, however, that the UK will continue to do so once it withdraws from the EU". Post-Brexit, the UK's rather sizeable influence over European sanctions policy will naturally diminish. The UK will also no longer be bound by European law and, without an agreement to the contrary, EU instruments such as EU Council Decisions and Regulations, will lose their legal force in the UK subject to the terms of the EU (Withdrawal) Act 2018. UN sanctions measures, however, will have to be implemented directly by the UK post-Brexit as the UK will continue to be bound by international law.

Current Implementation of UN and EU Sanctions in the UK

Currently, when sanctions are imposed by the UN or the EU, the UK acts on its international obligations to give effect to the sanctions in UK law. UN sanctions are implemented by the EU and, once implemented through EU regulation, they take direct legal effect in the UK.

At a domestic level, the UK makes statutory instruments (UK regulations) to criminalize breaches of financial sanctions and to impose penalties for breaches of EU regulations. Currently, the UK's domestic sanctions regime (as opposed to the international and regional sanctions regime created by the UN and the EU respectively)is confined to terrorism legislation and the

UK can only impose its own financial sanctions and restrictions under specific legislation, namely: The Anti-Terrorism Crime and Security Act 2001 ('ATCSA 2001'), the Counter Terrorism Act 2008 ('CTA 2008'), and the Terrorist Asset-Freezing Act 2010 ('TAFA 2010').

Following its departure from the EU, however, the UK will be at risk of breaching its international obligations if a way forward is not agreed. With that in mind, the UK Parliament has passed the Sanctions and Anti-Money Laundering Act 2018 ('SAMLA'), which received royal assent on 23 May 2018. This piece of legislation, which is anticipated to come into force at the time of the UK's departure from the EU, will fill the legislative lacuna created by Brexit and will enable the UK to impose sanctions for the first time, independently of the European community. Until SAMLA's provisions come into force, the UK's domestic sanctions regimes remain confined to terrorism legislation.

Deal or No Deal

In the event of a deal between the EU and UK, sanctions regulations will be among the many EU rules that the UK will continue to follow until the end of a so-called 'transition period' (even if it will play no part in helping to make them). This transition period will last for at least a year, and after it has run, the UK and EU will have made a decision as to how sanctions will apply. This decision will likely be made well in advance of the deadline so as to give businesses and financial professionals time to prepare for the switch.

On the other hand, if the UK departs from the EU without a deal, the majority of EU sanctions designations will be carried over and take effect under the SAMLA provisions in order to replace the existing EU regimes and through the EU Withdrawal Act which converts the EU regulations into domestic law as at the moment of exit.

Implementation of UN and EU Sanctions in the UK, Post-Brexit

SAMLA provides the UK with a domestic framework of powers to continue to meet its international obligations under the UN Charter by implementing UN sanctions directly in the UK and is designed to fill the legislative gap created by the UK leaving the EU. Among other things, it implements a new sanctions framework for the UK post-Brexit and enables the UK to use sanctions to meet national security and foreign policy objectives.

As to EU sanctions, it is likely that EU sanctions measures will also be transposed into UK law. According to the EU Withdrawal Act 2018, the current sanctions regimes in effect on the date of the UK's departure from the EU will form part of domestic law on and after exit day.

The Broad Scope of SAMLA

Though it is uncertain how its power will be used, SAMLA gives UK ministers rather broad powers to impose sanctions.

Section 1 of SAMLA gives effect to the very heart of the issue by empowering the Secretary of State and the Treasury to impose sanctions regulations that a minister considers 'appropriate' for purposes including: (a) complying with a UN obligation; and (b) to achieve a particular purpose including furthering the prevention of terrorism both in the UK and elsewhere; the interests of national security; furthering a foreign policy objective of the UK government; and promoting respect for democracy, the rule of law and good governance.

The contrast between current EU law and the new legislation is marked, not least because making a sanctions regulation on that basis that a Minister feels it is 'appropriate' is a lower threshold than the EU's regime 'necessity' test. The government's reassurances that it does not intend to alter how sanctions are implemented in practice does nothing to change the fact that the framework gives far greater discretion to the Minister, with the result that sanctions may be used more extensively than before.

A Change in Due Process

Currently, persons designated pursuant to UN sanctions are able to challenge their designations through the EU General Court, which affords them certain rights. Under SAMLA, however, individual rights will be reduced, and those on the UN list will be deprived of the rights they enjoy under EU law. For example, the EU General Court can declare designations unlawful even where they originate from UN Security Council decision. This is not an option under SAMLA. In other words, there is no judicial review process of UN sanctions measures in the UK.

SAMLA does provide a mechanism whereby a person designated on a UN sanctions list may request the Secretary of State to use his best endeavours to secure that the person's name is removed from the relevant UN list (Section25(2)). There remains, nevertheless, a distinction between domestic designations and UN designations, whereby the former are subject to judicial review but the latter are not.

The Future of UK Sanctions

The UK's legislative sanctions framework is permeated with uncertainty due to the international forces and obligations at play.

The UK has historically played a vital role in the design and implementation of EU sanctions, which is unlikely to continue once it withdraws from the EU.

On the other hand, the UK's departure from the EU is unlikely to change the UK's sanctions policy to any great extent, exactly because of its previous leadership role in sanctions proposals within the EU.

The government has confirmed that SAMLA, despite its far-reaching provisions, is not intended to alter the UK's substantive approach to sanctions. Nonetheless, the statute's provisions represent an overhaul and potential extension of the UK's sanctions framework. Notwithstanding the criticisms of SAMLA during its first readings, where it was said that it could lead to "a constitutional car crash" or a "bonanza of regulations", in practice, very little is likely to change. Moreover, a non-aligned approach between the UK and EU would carry significant risks for the UK itself, not least the likely backlash from EU member states who may see any significant divergence as an attempt to gain an unfair competitive advantage.

Some commentators have referred to the new institutional formula of EU 27+1 in shaping and co-implementing sanctions. For now, this is the most likely outcome so that the EU can reduce the risk that its weapon of choice be partially disarmed whilst protecting the UK's credibility as a global player.

United States

The United States is the most aggressive user of economic sanctions in the world, and the U.S. sanctions regime is especially complex and detailed. The United States utilizes sanctions to achieve a number of objectives, lie preventing certain types of activities, such as terrorism, narcotics trafficking, and weapons proliferation, and punishing violations of human rights, democracy, and the rule of law. It also uses sanctions to achieve foreign policy goals, although those goals are usually described in terms of preventing terrorism, weapons proliferation, etc. Each of the different sets of sanctions is referred to as a "program." While most programs, including those that appear to address whole countries, are directed only at individuals or entities, several countries, including Cuba, Iran, North Korea, and Syria, are subject to broad embargos. The United States also imposes sanctions against a number of different types of individuals and organizations, including terrorists, narcotics dealers, and weapons proliferators. The United States is unique in that some of its sanctions programs purport to require compliance by non-U.S. individuals and entities, giving them extraterritorial effect.

Like the European Union, the United States has three general approaches to sanctions: list based, country based, and sectoral. All individuals, and most (but not all) entities subject to sanctions are identified in specific lists. In addition, the United States imposes sanctions against entire countries in the cases of Cuba, Iran, North Korea, and Syria, and broad but not comprehensive sanctions against Russia and Venezuela. The United States formerly had broad sanctions against Burma (Myanmar) and Sudan, but these have mostly been removed. While sanctions against individuals and entities tend to be uniform, sanctions against countries can vary significantly in what they do and do not allow.

The sanctions laws are connected to, but legally apart from, the U.S. export control laws. Sanctions laws are administered and enforced primarily by the **Office of Foreign Assets Control ("OFAC")**.

OFAC

OFAC is a small agency within the U.S. Department of Treasury. It acts under Presidential wartime and national security authorities as well as authority granted under specific legislation. OFAC administers and enforces U.S. economic sanctions based on U.S. foreign policy and national security goals.

> OFAC is the agency primarily charged with administering and enforcing economic sanctions on behalf of the government of the United States

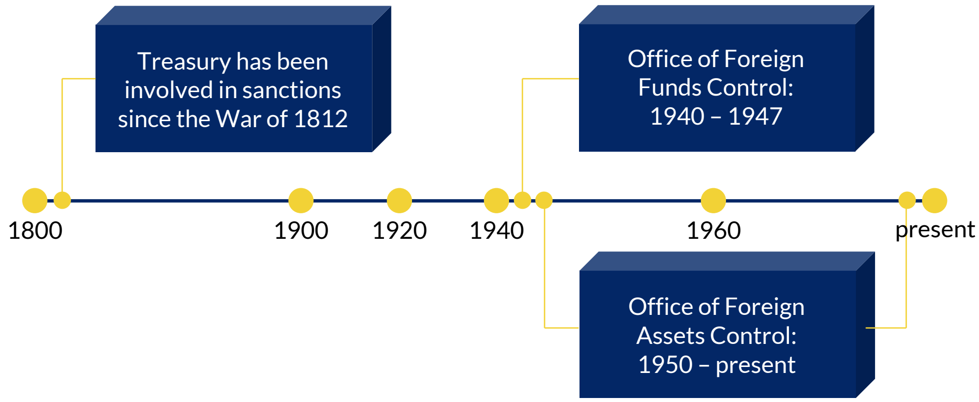
OFAC administers over 20 sanctions programs, all with a foreign focus / nexus. There has been unprecedented enforcement in recent years following increase of statutory penalties.

> OFAC targets:
> - Foreign countries and regimes
> - Non-state actors like terrorists, international narcotics traffickers, WMD proliferators, indicted war criminals, or transnational criminal organizations
> - And the support networks affiliated with these targets

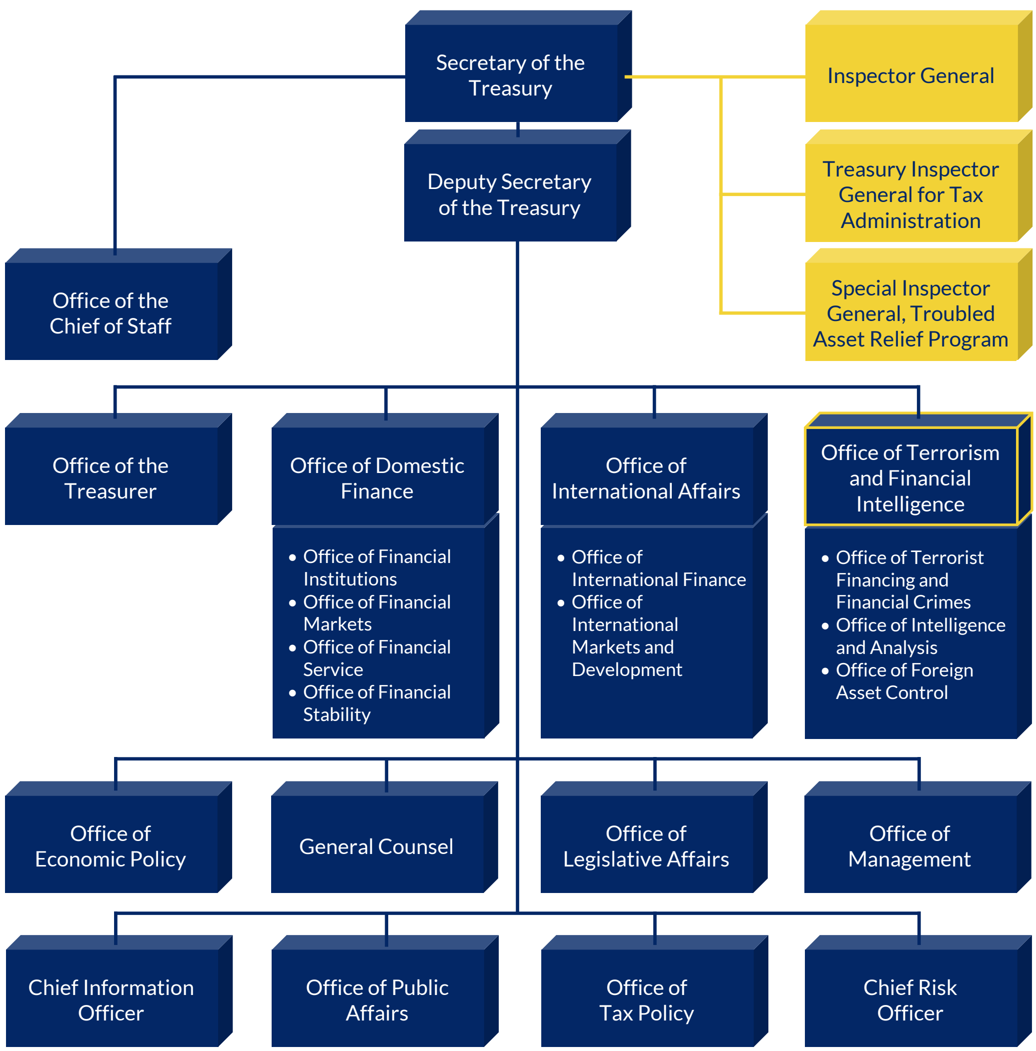
OFAC is the successor to the Office of Foreign Funds Control (the ``FFC''), which was established at the advent of World War II following the German invasion of Norway in 1940. The FFC program was administered by the Secretary of the Treasury throughout the war. The FFC's initial purpose was to prevent Nazi use of the occupied countries' holdings of foreign exchange and securities and to prevent forced repatriation of funds belonging to nationals of those countries. These controls were later extended to protect assets of other invaded countries. After the United States formally entered World War II, the FFC played a leading role in economic warfare against the Axis powers by blocking enemy assets and prohibiting foreign trade and financial transactions.

OFAC itself was formally created in December 1950, following the entry of China into the Korean War, when President Truman declared a national emergency and blocked all Chinese and North Korean assets subject to U.S. jurisdiction.

When Did OFAC Get Started?



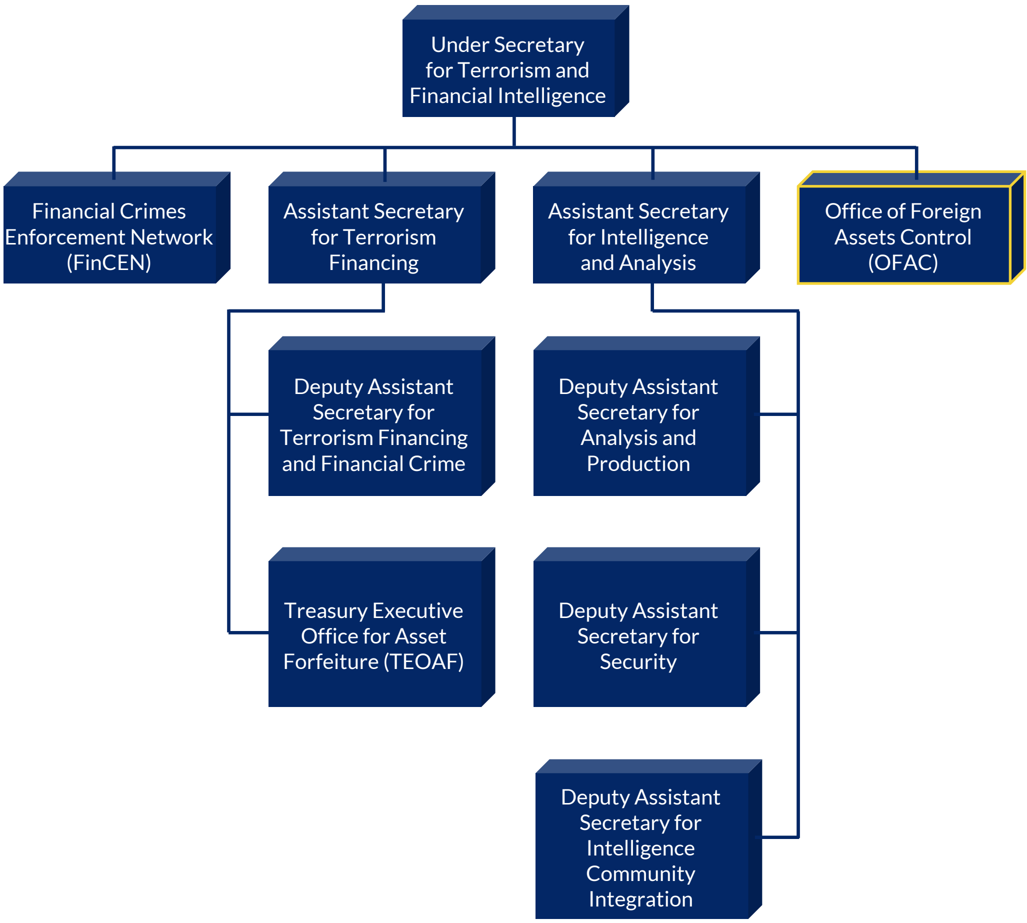
OFAC is inside the Department of the Treasury, in particular inside the Office of Terrorism and Financial Intelligence. Below is a chart that shows where it fits in the organizational structure.



As you can see, OFAC is inside the Office of Terrorism and Financial Intelligence (TFI).

The main goal of TFI is to sever the lines of financial support to international terrorists, WMD proliferators, narcotics traffickers, money launderers, and other threats to the U.S. national security.

Below is an org chart of TFI:



As you can see, another agency inside TFI, on the left, is FinCEN, the Financial Crimes Enforcement Network.

The **Bureau of Industry and Security ("BIS"),** an agency within the Department of Commerce, administers most U.S. export control laws. The State Department regulates exports of arms. The State Department may also play a role in designating individuals or entities as targets for sanctions. Along with OFAC, the Department of Justice is involved in enforcement of the sanctions laws, especially if a violation rises to the level of a crime. Finally, the Federal Reserve to some extent oversees and enforces sanctions compliance by banks.

Legal Basis

The legal basis for the imposition and enforcement of economic sanctions in the United States is Article I of the U.S. Constitution, which gives Congress the power to regulate commerce with foreign nations. The Constitution reserves this power to Congress, so that practically all U.S. sanctions law is federal in nature. Individual states do have sanctions laws, but these primarily limit the ability of state bodies, such as pension funds, to make certain types of investments.

Congress has in turn passed a number of statutes that impose specific sanctions and, more generally, delegates broad powers to the President (and, through him, the agencies of the Executive Branch) to impose and enforce sanctions. The two main statutes that confer on the President the broad ability to impose sanctions include

1. **Trading with the Enemy Act (TWEA).** TWEA, which dates back to 1917, gives the President the authority to prohibit or regulate trade, investments, remittances, travel and virtually any other economic transactions with any designated country or its nationals. The U.S. sanctions against Cuba were based on TWEA.
2. **International Emergency Economic Powers Act (IEEPA).** IEEPA authorizes the President to declare national emergencies in response to a specific threat. Having declared an emergency, the President has the power, among other things, to regulate property belonging to foreign persons that is subject to the jurisdiction of the United States. Most country sanctions programs, as well as sanctions against individuals and entities, are imposed under the authority of IEEPA.

A number of other statutes impose sanctions on specific countries, as well as against other sanctions targets, including terrorists and drug kingpins. OFAC lists no fewer than 33 such statutes in all. The major statutes imposing sanctions, with their citation in the U.S. Code, include:

General: Trade Sanctions Reform and Export Enhancement Act of 2000 (22 U.S.C. §§ 7201-7211); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001

Cuba: Cuban Democracy Act of 1992 (22 U.S.C. §§ 6001-6010); Cuban Liberty and Democratic Solidarity (Libertad) Act of 1996 (22 U.S.C. §§ 6021-6091)

Iran: Iran Freedom and Counter-Proliferation Act of 2012; Iran Freedom Support Act (50 U.S.C. § 1701 note); Iran Sanctions Act of 1996, as Amended (50 U.S.C. § 1701 note); Iran Threat Reduction and Syria Human Rights Act of 2012; National

Defense Authorization Act For Fiscal Year 2012; Countering America's Adversaries Through Sanctions Act (CAATSA)

Nicaragua: Nicaragua Human Rights and Anticorruption Act of 2018

North Korea: North Korean Sanctions and Policy Enhancement Act of 2016; CAATSA

Russia: Sergei Magnitsky Rule of Law Accountability Act of 2012; Support For The Sovereignty, Integrity, Democracy, And Economic Stability Of Ukraine Act Of 2014; Ukraine Freedom Support Act Of 2014; CAATSA

Syria: Iran Threat Reduction and Syria Human Rights Act of 2012

Venezuela: Venezuela Defense of Human Rights and Civil Society Act of 2014

Terrorism: Antiterrorism and Effective Death Penalty Act of 1996 (8 U.S.C. § 1189); USA PATRIOT ACT; CAATSA

Weapons Proliferation: Sections 2797b-c of the Arms Export Control Act

Narcotics Trafficking: Foreign Narcotics Kingpin Designation Act (21 U.S.C. §§ 1901-1908)

Democracy, Human Rights, and the Rule of Law: Global Magnitsky Human Rights Accountability Act

The Process

Sanctions can be imposed legally in several different ways. These include statutes, Executive Orders, and regulations. In addition, while they do not have the force of law, agency guidance, including Frequently Asked Questions, can essentially impose sanctions and create requirements for compliance as well.

Statutes

Statutes are measures enacted by Congress and signed into law by the President. Statutes are superior to all other forms of law except the Constitution. Statutes can impose sanctions directly. Section 103 of Cuban Liberty and Democratic Solidarity (Libertad) Act of 1996, for example, directly prohibits U.S. persons[3] from providing indirect financing for certain types of transactions involving Cuba. Such a direct imposition of sanctions by statute is relatively uncommon, though.

More common is for the statute to require the President to act in certain circumstances. In such cases, the statutory language will typically state that "the

[3] The definition of "U.S. person" is discussed below in the section on who must comply with U.S. sanctions

President shall impose" sanctions under the designated conditions. Section 228 of CAATSA, for example, states that

> The President shall impose the sanctions described in subsection (b) with respect to a foreign person if the President determines that the foreign person, based on credible information, on or after the date of the enactment of this section—
>
> "(1) is responsible for, complicit in, or responsible for ordering, controlling, or otherwise directing, the commission of serious human rights abuses in any territory forcibly occupied or otherwise controlled by the Government of the Russian Federation;

Under a provision like this, Congress does not itself designate the persons subject to sanctions. However, if the President who determines that a foreign person has engaged in the prescribed conduct and imposes sanctions. This will normally be done by an announcement by OFAC that an identified person has been designated as a Specially Designated National, and is subject to the sanctions set forth in the statute. Even if the imposition of sanctions is mandatory, though, statutes normally include a provision allowing the President to waive action, usually if doing so is necessary for national security. The statute may also include exceptions to the imposition of even mandatory sanctions.

A statute may also commit action to the President's discretion. In such cases, the statute usually provides that "the President may impose" sanctions. Section 232 of CAATSA provides an example:

> The President, in coordination with allies of the United States, may impose five or more of the sanctions described in section 235 with respect to a person if the President determines that the person knowingly, on or after the date of the enactment of this Act, makes an investment described in subsection (b) or sells, leases, or provides to the Russian Federation, for the construction of Russian energy export pipelines, goods, services, technology, information, or support described in subsection (c)—….

In this case, the imposition of sanctions is not mandatory. When confronted with evidence that a person has made an investment described in the statutory section, the President decides whether or not to impose sanctions. In addition, the statute gives the President discretion to determine which sanctions to apply. Consequently, the President has some freedom in deciding whether and how to act.

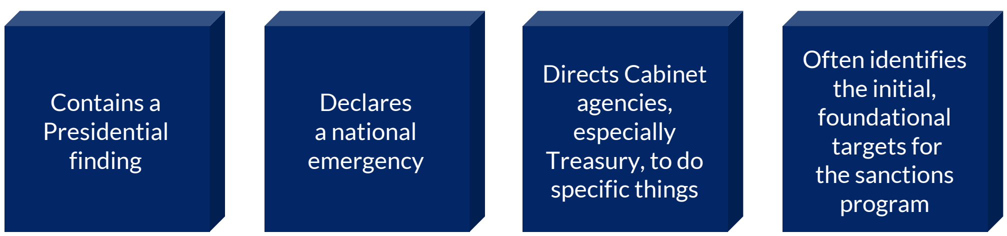
Finally, as discussed above, TWEA and especially IEEPA give the President broad authority to declare a national emergency with respect to a specific threat and to take appropriate measures, including the restriction or prohibition of transactions and the freezing of property. Sanctions against many countries, are imposed under the authority of IEEPA and other, more country-specific statutes.

Executive Orders

The immediate legal authority for the imposition of sanctions usually takes the form of an Executive Order issued by the President. While an Executive Order must be based on power delegated to the President by a statute, Congress does not review or approve Executive Orders (although it can overturn them by statute). As a consequence, the President can interpret, modify, and withdraw Executive Orders without any action by Congress. As a practical matter, most U.S. sanctions are imposed pursuant to an Executive Order.

An Executive Order begins with a citation to the statutory authority giving the President the right to act. The order then typically gives the President, the Secretary of the Treasury, or the Secretary of State the power to prohibit transactions and impose sanctions on individuals and entities. In some cases, the imposition of sanctions may be mandatory, in others discretionary. The Executive Order may also authorize the President or the Secretaries to take one or more actions.

Four Main Elements of E.O.



Executive Order13849 of September 20, 2018 is a typical example. It implements the imposition of sanctions against persons and entities in the Russian Federation under CAATSA:

> Section 1. (a) When the President, or the Secretary of State or the Secretary of the Treasury pursuant to authority delegated by the President and in accordance with the terms of such delegation, has determined that sanctions shall be imposed on a person pursuant to sections 224(a)(2), 231(a), 232(a), or 233(a) of CAATSA and has selected from section 235 of CAATSA any of the sanctions set forth below to impose on that person, the Secretary of the Treasury, in consultation with the Secretary of State, shall take the following actions where necessary to implement the sanctions selected and maintained by the President, the Secretary of State, or the Secretary of the Treasury:

i. prohibit any United States financial institution from making loans or providing credits to the sanctioned person totaling more than $10,000,000 in any 12-month period, unless the person is engaged in activities to relieve human suffering and the loans or credits are provided for such activities;
ii. prohibit any transactions in foreign exchange that are subject to the jurisdiction of the United States and in which the sanctioned person has any interest;
iii. prohibit any transfers of credit or payments between financial institutions, or by, through, or to any financial institution, to the extent that such transfers or payments are subject to the jurisdiction of the United States and involve any interest of the sanctioned person;
iv. block all property and interests in property of the sanctioned person that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person, and provide that such property and interests in property may not be transferred, paid, exported, withdrawn, or otherwise dealt in;
v. prohibit any United States person from investing in or purchasing significant amounts of equity or debt instruments of the sanctioned person; or
vi. impose on the principal executive officer or officers of the sanctioned person, or on persons performing similar functions and with similar authorities as such officer or officers, the sanctions described in subsections (a)(i)–(a)(v) of this section, as selected by the President, the Secretary of State, or the Secretary of the Treasury.

Three aspects of an Executive Order like this are noteworthy. First, the President or one of the Secretaries decides whether a person is subject to the sanctions set forth in CAATSA. Although the Order states that the President or the Secretaries "shall" act in such a case, it is left to them to decide what actions are necessary to enforce the sanctions. Finally, they can decide which sanctions to apply. This leaves the President a great deal of flexibility in deciding who to impose sanctions on, and what sanctions to impose.

A recent development has been the use of a statute to codify sanctions imposed under Executive Orders by the President. While the President could normally modify or revoke sanctions imposed under Executive Orders, the codification of such sanctions means that Congressional action is required to make any changes.

Regulations

Both statutes and Executive Orders tend to impose sanctions in fairly broad terms. The actual administration of sanctions, however, usually requires a greater level of detail. This is provided in the form of regulations issued by OFAC. Indeed, an Executive Order may direct OFAC to promulgate regulations with respect to a particular sanctions program. A typical regulation, such as the Iranian Transactions and Sanctions Regulations (included in the Appendix) will cover

1. Prohibited transactions (imports, exports, investments, dealing in blocked property, etc.)
2. Definitions
3. Interpretations
4. Licenses and exemptions
5. Reporting requirements
6. Penalties for violations

A single program may have multiple sets of regulations, covering different aspects of the program. Regulations do not normally provide the authority to designate persons as being subject to sanctions, though; this is usually done through an Executive Order.

Agency Guidance and FAQs

Even regulations cannot necessarily provide all of the detail needed to interpret and apply U.S. sanctions. OFAC accordingly publishes guidance (sometimes called interpretive guidance) on a variety of issues. Some are general in nature, such as the ability of U.S. attorneys to provide sanctions advice to non-U.S. persons, while others provide commentary on specific issues with individual sanctions programs.

In addition, OFAC has published responses to a number of frequently asked questions (FAQs); at last count, there were 690 of these. These FAQs address everything from the broadest of questions ("what is OFAC and what does it do?") to the very specific ("what is the definition of the copper sector of Iran?"). These FAQs can be found at https://www.treasury.gov/resource-center/faqs/Sanctions/Documents/faq_all.html.

Guidance, interpretive guidance, and FAQs do not have the force of law. However, they do reflect OFAC's interpretation of statutes, Executive Orders, and regulations, as well as OFAC's conclusions regarding the responsibility of U.S. persons and others for compliance with U.S. sanctions laws. In the United States, courts traditionally give great deference to an agency's interpretation of the laws.

Finally, anyone can request advice from OFAC on either broad topics, or on whether a particular transaction would violate U.S. law. While OFAC's response is not necessarily binding, such a response is again a strong indication of how the agency interprets and applies U.S. sanctions laws. For this reason, proceeding with a transaction that OFAC has indicated it believes is illegal may expose the parties to the transaction to a real risk of violating U.S. law.

United Nations Sanctions

The United States does not automatically apply UN sanctions. As a practical matter, however, the United States normally incorporates UN sanctions into domestic law very quickly. U.S. sanctions are much broader than those imposed by the UN, though.

Types of Sanctions

The types of sanctions used by the United States resemble those utilized by the EU. These sanctions include arms embargoes, trade sanctions, financial sanctions, travel bans, and asset freezes. Unlike the EU, U.S. sanctions tend to be much broader and less targeted, in the sense that several countries are subject to general embargos of trade and finance. The United States evinces less concern for the impact of sanctions on the population of countries subject to embargos, although certain exceptions and general licenses seek to mitigate at least some of the humanitarian damage caused by sanctions.

No single document contains all of the U.S. sanctions in force. The OFAC web site, however, contains comprehensive information on the U.S. sanctions under the various programs, including the applicable statutes, Executive Orders, regulations, guidance, and FAQs, as well as on general licenses. In addition, OFAC publishes summaries of the various sanctions programs. While these provide useful overviews, they are not always up-to-date. OFAC does operate an e-mail list whose participants are informed of any changes to U.S. sanction the day they occur. OFAC maintains a comprehensive list of all of its "recent actions" containing updates, changes in laws, and penalty notices, at https://www.treasury.gov/resource-center/sanctions/ofac-enforcement/pages/ofac-recent-actions.aspx. A subscription to OFAC's e-mail service for recent actions is available on the same page.

Blocking of Property is the most sweeping sanction applied by the United States. In this sense, "blocking" essentially means freezing the goods or services. This sanction is applied to individuals, entities, or others that have been designated by OFAC as "Specially Designated Nationals," or SDNs. It may also be applied to entire governments, as is currently the case with North Korea, Syria, and Venezuela. Executive Order 13884, which applied this sanction to the Government of Venezuela, employs typical language:

> Section 1. (a) All property and interests in property of the Government of Venezuela that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in.

The terms "property" and "interest in property" encompass practically anything of value, as the definition from the ITSR shows:

> The terms property and property interest include, but are not limited to, money, checks, drafts, bullion, bank deposits, savings accounts, debts, indebtedness, obligations, notes, guarantees, debentures, stocks, bonds, coupons, any other financial instruments, bankers acceptances, mortgages, pledges, liens or other rights in the nature of security, warehouse receipts, bills of lading, trust receipts, bills of sale, any other evidences of title, ownership or indebtedness, letters of credit and any documents relating to any rights or obligations thereunder, powers of attorney, goods, wares, merchandise, chattels, stocks on hand, ships, goods on ships, real estate mortgages, deeds of trust, vendors' sales agreements, land contracts, leaseholds, ground rents, real estate and any other interest therein, options, negotiable instruments, trade acceptances, royalties, book accounts, accounts payable, judgments, patents, trademarks or copyrights, insurance policies, safe deposit boxes and their contents, annuities, pooling agreements, services of any nature whatsoever, contracts of any nature whatsoever, and any other property, real, personal, or mixed, tangible or intangible, or interest or interests therein, present, future, or contingent.

Blocked property remains under the ownership of the sanctioned person or entity; the U.S. government has not seized the property. U.S. persons who gain control over funds belonging to a sanctioned person are required to place those funds in a separate interest-bearing account. The funds cannot be withdrawn or disbursed without the permission of OFAC. Similarly, if physical assets are involved, those assets must be maintained at the expense of the owner (i.e., the sanctioned party), although OFAC can allow their liquidation and the deposit of the resulting funds in an interest-bearing account. Unlike the EU, U.S. sanctions do not contain any fixed exceptions allowing for access to blocked property, although OFAC may always do so by issuing a license.

Travel bans consist of restrictions or prohibitions on travel by designated individuals to the United States. Executive Order 13884, which imposed various sanctions on Venezuela, uses fairly standard language to impose a travel ban:

> The unrestricted immigrant and nonimmigrant entry into the United States of aliens determined to meet one or more of the criteria in section 1(b) of this order would be detrimental to the interests of the United States, and entry of such persons into the United States, as immigrants or nonimmigrants, is hereby suspended, except when the Secretary of State determines that the person's entry would not be contrary to the interests of the United States.

All immigration law in the United States is federal, so that such a travel ban applies throughout the United States. The United States may also ban travel by U.S. nationals to certain countries. Presently, such travel bans apply to Cuba (with some relatively significant exceptions) and to North Korea.

Arms embargoes prohibit the sale weapons and related services to restricted individuals, groups, or states. The U.S. "Munitions List" designates various goods, services, and technology as being defense articles or services. Exports of items on the Munitions List require a license from the State Department, which may act on the advice of the Department of Defense. The Munitions List covers 20 different categories of articles, services, and technology, including firearms; guns; ammunition; missiles, rockets, bombs, and mines; explosives; naval vehicles; military ground vehicles; military aircraft; military training equipment; personal protective equipment; military electronics; fire control and guidance equipment; various other materials; chemical and biological agents; spacecraft; nuclear weapons; directed energy weapons; gas turbine engines; and submarines. Whether a given product is on the Munitions List may depend upon its precise characteristics. The Munitions List explicitly includes not just military articles, but the services and technology associated with those articles.

The Munitions List is incorporated into the International Trade in Arms Regulations ("ITAR"). ITAR is administered by the Directorate of Defense Trade Controls (DDTC), an agency within the State Department. DDTC must license all exports of goods, services, or technology on the Munitions List in advance. Exports of defense items to Belarus, Burma (Myanmar), China, Cuba, Iran, North Korea, Syria, and Venezuela are completely. Exports to Afghanistan, Central African Republic, Cyprus, Democratic Republic of Congo, Eritrea, Haiti, Iraq, Lebanon, Libya, Somalia, South Sudan, Sudan, and Zimbabwe, are generally prohibited, but there are narrow exceptions. Exports of defense items to Russia are not prohibited per se, but are subject to very tight controls. Conversely, U.S. law also prohibit imports of defense materials from some countries, such as Russia.

Restrictions on imports, exports, and investment.

U.S. sanctions directed against countries that go beyond the designation of individuals or entities as SDNs almost always contain some sort of prohibition on imports, exports, and investment.

Imports

The legal language prohibiting imports tends to be quite straightforward. The Iranian Transactions and Sanctions Regulations (ITSR), for example, contain the following provisions:

> §560.201 Prohibited importation of goods or services from Iran.
>
> Except as otherwise authorized pursuant to this part, and notwithstanding any contract entered into or any license or permit granted prior to May 7, 1995, the importation into the United States of any goods or services of Iranian origin or owned or controlled by the Government of Iran, other than information and informational

> materials within the meaning of section 203(b)(3) of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)(3)), is prohibited.

There may be exceptions for specific imports. The U.S. sanctions against Iran previously allowed the importation of Persian carpets and pistachios from Iran, although these exceptions were removed when the United States reimposed broad sanctions against Iran in 2017.

Exports

The language of ITSR prohibiting exports is even broader:

> §560.204 Prohibited exportation, reexportation, sale, or supply of goods, technology, or services to Iran.
>
> Except as otherwise authorized pursuant to this part, and notwithstanding any contract entered into or any license or permit granted prior to May 7, 1995, the exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any goods, technology, or services to Iran or the Government of Iran is prohibited, including the exportation, reexportation, sale, or supply of any goods, technology, or services to a person in a third country undertaken with knowledge or reason to know that:
>
> (a) Such goods, technology, or services are intended specifically for supply, transshipment, or reexportation, directly or indirectly, to Iran or the Government of Iran; or
>
> (b) Such goods, technology, or services are intended specifically for use in the production of, for commingling with, or for incorporation into goods, technology, or services to be directly or indirectly supplied, transshipped, or reexported exclusively or predominantly to Iran or the Government of Iran.

U.S. export sanctions include services and technology as well as goods. Financial services are considered a form of services, so that a ban on the export of services essentially prevents any transactions with the target country, as no U.S. bank can process the transaction. Technology includes software, preventing sales over the Internet as well. Sanctions apply to exports to the government of the target country as well as to the territory of the target country.

As well as banning exports from the United States or by U.S. persons, U.S. sanctions may also prohibit the re-exportation of U.S. goods, services, or technology by non-U.S. persons:

> §560.205 Prohibited reexportation of goods, technology, or services to Iran or the Government of Iran by persons other than United States persons; exceptions.
>
> (a) Except as otherwise authorized pursuant to this part, and notwithstanding any contract entered into or any license or permit granted prior to May 7, 1995, the reexportation from a third country, directly or indirectly, by a person other than a United States person, of any goods, technology, or services that have been exported from the United States is prohibited, if:
>
> (1) Undertaken with knowledge or reason to know that the reexportation is intended specifically for Iran or the Government of Iran; and
>
> (2) The exportation of such goods, technology, or services from the United States to Iran was subject to export license application requirements under any United States regulations in effect on May 6, 1995, or thereafter is made subject to such requirements imposed independently of this part (see §560.414).

The export prohibition applies to non-U.S. persons if they knew, when they purchased the items, that they were intended for exportation to Iran. The prohibition also includes U.S. -origin articles that are used in the production of or are incorporated into goods, technology, or services where, at the time of their purchase, the intent was to export the finished article to Iran.

These prohibitions commonly contain a de minimis requirements, so that the prohibition does not apply if the value of the U.S. content of the finished good, service, or technology is below a specified percentage. The percentage allowed varies by country; in the case of Iran, for example, it is less than 10 percent. The de minimis exception does not apply, however, to U.S.-origin goods that are subject to export controls; no exports of products containing such items are allowed without a license.

Finally, trade measures may restrict exports of goods, services, and technology to specific sectors or industries in the target country, while allowing other exports. An example is the prohibition on exports to certain energy projects in Russia, which is discussed below.

Trade-related Transactions

As well as prohibiting the import or export of goods, services, or technology, U.S. sanctions may prohibit U.S. persons from participating in essentially any way in a transaction involving a country subject to sanctions, as the following provision from the ITSR provides:

§560.206 Prohibited trade-related transactions with Iran; goods, technology, or services.

(a) Except as otherwise authorized pursuant to this part, and notwithstanding any contract entered into or any license or permit granted prior to May 7, 1995, no United States person, wherever located, may engage in any transaction or dealing in or related to:

(1) Goods or services of Iranian origin or owned or controlled by the Government of Iran; or

(2) Goods, technology, or services for exportation, reexportation, sale or supply, directly or indirectly, to Iran or the Government of Iran.

(b) For purposes of paragraph (a) of this section, the term transaction or dealing includes but is not limited to purchasing, selling, transporting, swapping, brokering, approving, financing, facilitating, or guaranteeing.

As the regulation makes clear, the definition of "transaction or dealing" is very broad, and encompasses any role a U.S. person could potentially take in a transaction involving a country subject to sanctions.

Investment

A less common type of economic sanction is a prohibition or restriction on investment. Unlike the EU, the United States usually prohibits all investment after a certain date. The following example is from the ITSR:

§560.207 Prohibited investment.

Except as otherwise authorized pursuant to this part, and notwithstanding any contract entered into or any license or permit granted prior to May 7, 1995, any new investment by a United States person in Iran or in property (including entities) owned or controlled by the Government of Iran is prohibited.

"Investment" in this sense includes a commitment or contribution of funds or other assets, or a loan or other extension of credit. Such a sanction does not technically require a U.S. person to liquidate existing investments, but it may make it impossible for them to provide any additional funds or assets. Sanctions against the export of financial services may also prevent them from receiving dividends or repatriating profits or capital from investments in countries subject to sanctions.

Menu Sanctions

Several U.S. sanctions statutes, including the Iran Sanctions Act and CAATSA, prescribe so-called "menu" sanctions as well. These sanctions are directed against persons who knowingly engage in certain types of activities, such as investment in or support for the Iranian petroleum sector. Under these provisions, the President can impose five or more of a number of different measures, including

- A prohibition on financing from the United States Export-Import Bank for exports to the sanctioned person;
- Denial of the issuance of licenses for exports from the United States to the sanctioned person;
- Prohibition on the provision of loans to the sanctioned person by U.S. banks;
- U.S. opposition to any loans from international financial institutions, such as development banks;
- Ban on the U.S. government procuring goods, services, or technology from the sanctioned person;
- Restrictions or prohibition on the acquisition of foreign exchange by the sanctioned person, i.e., a ban on the ability to use U.S. dollars;
- Restrictions or prohibitions on transactions involving property subject to U.S. jurisdiction;
- A prohibition on investment by U.S. persons in the debt or equity of the sanctioned person;
- Exclusion of corporate officers from the United States;
- Sanctioned against corporate officers.

In addition, financial institutions may be denied designation as a primary dealer in U.S. government bonds and use as a repository for U.S. government funds. The United States has in fact been very reluctant to actually apply these sanctions. They remain U.S. law, however, and this situation could change at any time.

Sanctions Against Foreign Financial Institutions

Some U.S. sanctions are directed specifically against foreign banks and other financial institutions. U.S. sanctions against Iran, North Korea, and Russia permit or require the President to impose sanctions against foreign financial institutions that engage in certain types of activities. These sanctions primarily take the form of restrictions or prohibition of the maintenance of correspondent and payable-through accounts by U.S. financial institutions in favor of the foreign bank. Such measures would essentially cut sanctioned foreign financial institutions off from access to the U.S. financial system.

Sectoral Sanctions

Like the EU, the United States also imposes sectoral sanctions against certain entities in Russia and Venezuela. There are two main types of sectoral sanctions:

Prohibition on dealing in debt and equity: U.S. persons are prohibited from dealing in debt or equity of a designated entity issued after a specified date. With respect to debt, the prohibition applies only if the debt has a maturity beyond a set limit. The applicable limit varies according to the sector in which the designated entity operates. "Dealing" encompasses virtually all possible actions in connection with debt or equity.

Restrictions on exports: U.S. persons are prohibited from exporting goods, services, or technology to designated Russia entities in connection with certain types of petroleum projects.

Evasion and Facilitation

While not strictly a sanction, U.S. law prohibits any transaction that "evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate" a U.S. sanction. Unlike some of the other prohibitions, this is not restricted to U.S. persons only, so that a foreign person who caused a violation of sanctions by, for example, concealing the presence of a sanctioned element in a transaction so that a U.S. bank processed the transaction, could itself violate sanctions.

U.S. sanctions law also prohibits U.S. persons from facilitating transactions if it would be illegal for them to participate in the transaction directly. Section 560.208 of the ITSR provides standard language banning facilitation:

{N}o United States person, wherever located, may approve, finance, facilitate, or guarantee any transaction by a foreign person where the transaction by that foreign person would be prohibited by this part if performed by a United States person or within the United States.

Facilitation is a poorly-defined concept, and could potentially reach almost any involvement in an otherwise-prohibited transaction at all. Among other actions, the ban on facilitation would prevent a U.S. person from referring a business opportunity or transaction involving a sanctioned person, entity, or country to a non-U.S. person. The prohibition on facilitation does apply only to U.S. persons.

Licenses and Exceptions

Certain types of transactions are normally exempted from U.S. sanctions. In addition, either a general or a specific license may authorize transactions that would otherwise be prohibited.

Exceptions and General Licenses

Because U.S. prohibitions on imports and exports regarding individual countries tend to be comprehensive, they commonly include a number of exceptions and exemptions. These may be statutory or provided for in regulation. Common exceptions and exemptions include

- Post and telecommunications
- Humanitarian donations
- Information and informational materials (including books, music, photographs, and film)
- Expenses associated with travel (where travel is allowed)
- Official business.

General licenses are similar to exceptions. Despite the name, they are available to all persons, and no application is required. General licenses may be provided for in a regulation or issued separately by OFAC. They may provide very broad authorizations, allowing exports of whole categories of products, or very specific, such as an authorization to engage in specified types of transactions with a named entity. General licenses may be open-ended or limited to a certain period.

Under the various country sanctions programs, general licenses generally authorize exports of agricultural products and medicine and medical products from bans on exports. The regulations regarding what qualify are quite specific. In addition, it may be necessary to follow a set procedure for such exports to qualify. Exports of permitted agricultural products to Cuba, for example, do not require a license as such, but BIS must be notified of the export before it occurs. If a transaction is exempted from sanctions, other transactions necessary to conduct it, such as financing or the processing of payments, are also allowed.

Specific Licenses

OFAC may also issue specific licenses. A specific license authorizes a designated party to engage in a transaction or series of transactions for a prescribed period of time. The license may also identify the individual entities otherwise subject to sanctions with which transactions can be conducted. The authorization provided by a specific license is available only to the licensee. For this reason, it is common for a license to identify, not just the individual party seeking the license, but any affiliates and subcontractors that may also be involved. Both U.S. and non-U.S. persons may apply for a license; the latter may occur when, for example, a non-U.S. company wishes to re-export U.S. origin products to a sanctioned country. The licensee must comply strictly with the terms of a license. OFAC will consider requests for renewal, but this requires the filing of a new license application.

OFAC accepts license applications through its online portal at https://licensing.ofac.treas.gov/Apply/Introduction.aspx. The same process is used to seek guidance regarding a potential transaction. While the online application form requests basic information, it is also possible to attach documents. It is usually best to include a letter providing the full details of the request. The application should identify:

1. The type of license sought (release of blocked wire transfers, Cuban travel, exports of certain agricultural or medical products to Iran or Sudan, a specific license for a transaction or series of transactions, or interpretive guidance regarding a potential transaction)
2. The applicable sanctions program or programs;
3. The names of any SDNs involved in the transaction;
4. The name and address of the applicant;
5. Why the applicant believes a license is necessary;
6. The purpose of the application;
7. A complete description of the contemplated transactions, including money flows and other related transactions;
8. The names of all potential parties to the transactions, including affiliates and subcontractors;
9. The length of time for which the license is sought; and
10. Include any appropriate documents, such as contracts, sales literature describing the goods involved, and copies of past licenses.

Targets of U.S. Sanctions

Targets of U.S. sanctions include individuals, legal entities, informal organizations such as Al Qaida, vessels, aircraft, governments, regions of countries, and countries. Sanctions targets are potentially subject to a range of different measures, from complete asset freezes to restrictions on the ability to borrow from U.S. persons or to use U.S. government programs.

SDNs

The most comprehensive U.S. sanctions apply to Specially Designated Nationals (SDNs)Pursuant to various statutes and Executive Orders, OFAC may designate individuals, legal entities, individual government agencies, vessels, and aircraft as SDNs. The reasons for which a person or entity may be designated an SDN include:

- Engagement in or support of international terrorism
- Narcotics trafficking
- Arms proliferation
- Assistance in the development of weapons of mass destruction
- Suppression of democracy, human rights, and the rule of law

As discussed above, U.S. persons are generally prohibited from having any dealings with SDNs, and are required to block any property or interest in property of an SDN that comes under their control. The names of SDNs are published on the SDN list, which is available at https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx in various formats. In addition, OFAC has created a search tool for determining whether a person or entity is on the SDN list.

The entry on the SDN list for each SDN provides the name and alternative names or aliases. For entities, it provides the address, as well as other relevant information, such as the commercial registry number. For individuals, the listing shows the date and place of birth, nationality, passport number, and other passport information. Finally, the SDN listing shows the sanctions programs under which the person or entity was designated, and whether they are potentially subject to secondary sanctions. Interestingly, the SDN list does not show the date of designation or the Executive Order or statute under which the designation was made.

As with the EU, entities owned by SDNs are also subject to U.S. sanctions laws, even if they have not been separately designated. Under U.S. law, any entity that is owned 50 percent or more by any combination of SDNs is also considered an SDN by operation of law. OFAC does not apply a control test. However, under its 50 percent rule, OFAC will examine the chain of ownership. If an SDN or combination of SDNs owns 50 percent or more of an entity, that entity is designated as a matter of law. In turn, all entities in which that entity has a 50 percent or greater ownership is also designated. This can continue through several stages. The following example shows how an entity in which an SDN owns a minority share could nonetheless be treated as an SDN as well:

1. SDN Z owns 51 percent of Company A. Company A is also an SDN.
2. Company A owns 51 percent of Company B. Company B is also an SDN because Company A owns 51 percent of it, even though SDN Z owns only 26 percent of it.

This chain could continue indefinitely. OFAC's guidance on the 50 percent rule is included in the Appendix.

Regions and Countries

Regions and countries can also be the target of OFAC sanctions. At present, Cuba, Iran, North Korea, and Syria are subject to comprehensive or near-comprehensive sanctions that ban most transactions between the United States and U.S persons and these countries. In some cases, the United States has also frozen property belonging either to the governments of these countries, or to individual government agencies or entities. The United States has also imposed an embargo on economic relations with the Crimea region of Ukraine following its purported annexation into the Russian Federation. The United States maintains broad but not comprehensive sanctions against Russia and Venezuela, although sanctions against both have expanded over time. The U.S. sanctions involving the Darfur region of Sudan are directed at persons and entities committing massive human rights violations in Darfur, rather than at the Darfur region itself.

Sectoral Sanctions Identifications

The United States imposes sectoral sanctions against certain designated companies in the finance, energy, and defense sectors of the Russian economy. These entities are designated as Sectoral Sanctions Identifications (SSIs). As with SDNs, entities that are owned 50 percent or more by SSIs are also subject to sectoral sanctions, even if they are not separately included in the SSI List.

U.S. law prohibits U.S. persons from dealing in the debt or equity of SSIs under certain circumstances, as well as exporting goods, services, or technology to SSIs in connection with certain petroleum projects in Russia. SSIs are subject only to the prescribed sanctions, and all other transactions with SSIs are legal. There is no requirement (or indeed, legal basis) to block their property.

The Sectoral Sanctions Identifications List, which can be found at https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/ssi_list.aspx.

Foreign Sanctions Evaders

Executive Order 13608, "Prohibiting Certain Transactions With and Suspending Entry Into the United States of Foreign Sanctions Evaders With Respect to Iran and Syria" gives OFAC the authority to impose sanctions on foreign persons (individuals and entities) who OFAC determines (1) to have violated, attempted to violate, conspired to violate, or caused a violation of U .S. sanctions concerning Syria or Iran, or (2) to have facilitated deceptive transactions for or on behalf of persons subject to U.S. sanctions concerning Syria or Iran. U.S. persons are basically prohibited from having any dealings with Foreign Sanctions Evaders. Unlike SDNs, though, there is no requirement to block their property.

Foreign Financial Institutions

Foreign financial institutions can be subject to U.S. sanctions if they conduct certain types of transactions involving Iran, North Korea, Russia, or Syria. These institutions are identified in the so-called CAPTA (Correspondent Account Payable Through Account List). At present, only one financial institution, the Bank of Kunlun in China, is on this list.

Secondary Sanctions

U.S. law allows for the imposition of a range of sanctions against foreign persons and entities that engage in certain types of transactions with Iran, North Korea, Russia, and Syria. These sanctions range from the menu sanctions described above to mandatory designation as an SDN. Individuals and entities with whom transactions can give rise to secondary sanctions are identified as such in the SDN list.

Potentially any individual or entity in the world, other than U.S. persons, could accordingly be subject to secondary sanctions. Although U.S. law has had provisions regarding secondary sanctions in place for some time, the United States has in fact been extremely reluctant to apply them, for political and economic reasons. Nonetheless, their existence means that foreign persons who do business with Iran, North Korea, Russia, or Syria should be aware of these sanctions, and the fact that this business could result in the imposition of sanctions upon them.

Below is a chart that highlights the differences between primary and secondary sanctions.

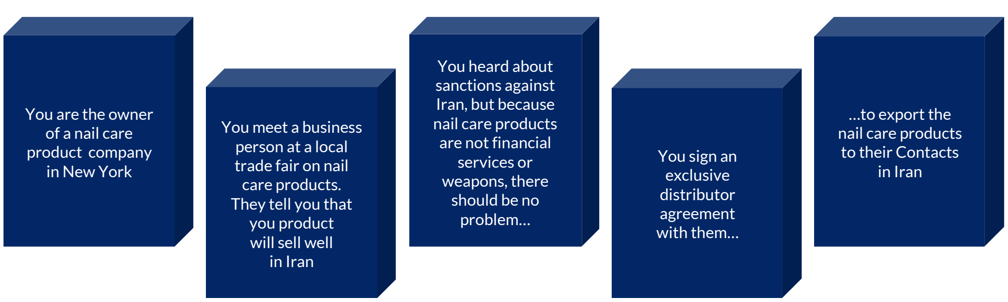
	Primary Sanctions	Secondary Sanctions
Since	1812	2010
Goal	Seek to regulate behavior of US persons	Influence the actions of non US persons
What they do	They require US persons to block assets within their possession or control or to prohibit US persons from engaging in transactions with the targets of sanctions.	Threaten non-US persons with becoming OFAC sanctions targets themselves if they continue to deal with specific, existing targets of US sanctions

Who Must Comply with U.S. Sanctions?

As a general rule, U.S. sanctions apply to "U.S. persons." U.S. persons include U.S. citizens and resident aliens, wherever they are located. They also apply to entities organized under the laws of a state, even if they are doing business abroad. Branches of U.S. companies in other countries are considered U.S. persons as well. U.S. subsidiaries of foreign companies are U.S. persons.

The below scenario highlights the fact that OFAC's reach goes beyond financial institutions:

Scenario



You may think that this is a hypothetical scenario. It is not. Keep on reading:

Scenario with Real Life Lesson

The scenario you just saw is adapted from a real life. It turns out that a lot can go wrong!

Even innocuous products or services can become involved in OFAC violations if they are exported to a sanctioned country.

A New York cosmetics firm learned this the hard way. The company was fined $450,000 by OFAC for exporting nail care products to Iran.

ENFORCEMENT INFORMATION FOR (April 10, 2012)

ENTITIES – 31 CFR 501.805(d)(1)(i)

Essie Cosmetics Ltd. And Individual Corporate Officer Settle Iranian Transactions Regulations Allegations:

OFAC

Essie Cosmetics Ltd. ("Essie") and a former individual corporate officer ("Individual"), New York City, New York, have agreed to settle OFAC allegations involving Essie and Individual's unlicensed exports to Iran in violation of the Iranian Transactions Regulations (the "ITR"), promulgated pursuant to, inter alia, the International.

Foreign subsidiaries of U.S. companies – i.e., those organized under the law of another country – are not considered U.S. persons. As a consequence, foreign subsidiaries may be able to do some types of business that their U.S. parents could not. However, the sanctions laws regarding Cuba and Iran specify that they apply to foreign subsidiaries of U.S. companies as well. It is this requirement that gave rise to the EU blocking statute. Even if a foreign subsidiary is legally permitted to do business with sanctioned entities or countries, though, any involvement of the U.S. parent in a transaction could expose the U.S. parent to liability.

U.S. sanctions also apply to any person who is physically present in the territory of the United States, regardless of their nationality. This remains true as long as they are present in the United States. Similarly, U.S. sanctions laws apply to any business a foreign entity does in the United States, even if it has no physical presence in the United States.

U.S. sanctions laws also effectively apply to all transactions denominated in U.S. dollars. If any segment of a transaction involves a U.S. person, it is subject to U.S. law. Practically all non-cash U.S. dollar payments are cleared through U.S. banks, which are U.S. persons. Even if no other party to the transaction is a U.S. person, the involvement of a U.S. bank or any other U.S. person in the transaction will result in the potential application of U.S. law.

U.S. Sanctions Programs

The United States currently has in place 31 different sanctions programs. The scope of these programs vary widely. Most involve the designation of individuals and entities as SDNs in response to actions that undermine the goals of the program. To stress that sanctions are not directed at the country as a whole, many of these programs are described as “Related,” such as the Mali-Related Sanctions. Other of the country-related sanctions, though, are quite extensive, and in the cases of Cuba, Iran, North Korea, and Syria essentially impose an embargo. The programs, their purposes, and the sanctions they apply are summarized below:

Balkans-Related

These sanctions which were originally implemented in 2001, are directed at individuals and entities whose actions undermined efforts to establish stability in the Western Balkans, and especially in Bosnia-Herzegovina. Targets of these sanctions are designated as SDNs. There are no country-specific sanctions under this program.

Belarus

U.S. sanctions against Belarus are directed at individuals and entities who undermine Belarus’ democratic processes or institutions, commit human rights abuses related to political repression, and engage in public corruption including by diverting or misusing Belarusian public assets or by misusing public authority. The only sanctions imposed under this program are the designations of various Belarusan government officials, including President Lukashenka, as SDNs. Otherwise, all transactions with Belarus are allowed.

OFAC has designated a number of major state-owned companies as SDNs, including Belneftikhim, the state-owned oil and chemical company. Belneftikhim owns a large number of other countries in Belarus. Because of OFAC’s 50 percent rule, these companies are considered SDNs as well. To complicate things, it is not always easy to determine ownership in Belarus. OFAC has repeatedly issued a general license, however, authorizing U.S. persons to engage in transactions with a number of major Belarusan SDNs, including Belneftikhim. These general licenses have had a term of six months. Although they have been regularly renewed, there is always the possibility that OFAC will either decline to renew the license, or even revoke it.

Burundi Sanctions

Under the Burundi sanctions, the United States has designated as SDNs a number of individuals, including present and former government officials, for actions undermining democracy and human rights in Burundi. Otherwise, all transactions with Burundi are allowed.

Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA)

CAATSA imposes sanctions against a number of countries, including Iran, North Korea, Syria, and Russia. OFAC nonetheless treats certain sanctions provided for under CAATSA as a separate sanctions program. These sanctions will be discussed in the context of the individual countries below.

Central African Republic

Under these sanctions, OFAC designates as SDNs persons whose actions undermine the peace and security of the Central African Republic. All other transactions with the CAR are allowed.

Counter Narcotics Trafficking

This program applies sanctions significant foreign narcotics traffickers and their organizations worldwide. Narcotics traffickers may be designated as SDNs. Companies and entities they own or control may also be designated.

Counter Terrorism

The suppression of terrorism is a major U.S. foreign policy goal. The primary sanction under this program is the designation of individuals and entities who commit terrorist acts or support terrorism as SDNs.

Cuba

Cuba is the oldest sanctions program of the United States. The United States imposed a general embargo against Cuba in 1960. Although there have been some changes, the United States continues to maintain a comprehensive embargo on trade, financial, and travel transactions with Cuba.

Coverage: Unlike other U.S. sanctions programs, the Cuban program does not use the term “U.S. person.” Rather, it covers “persons subject to U.S. jurisdiction,” which is defined as

a. Any individual, wherever located, who is a citizen or resident of the United States;
b. Any person within the United States as defined in §515.330;

c. Any corporation, partnership, association, or other organization organized under the laws of the United States or of any State, territory, possession, or district of the United States; and
d. Any corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by persons specified in paragraphs (a) or (c) of this section.

Consequently, foreign subsidiaries of U.S. companies are subject to U.S. sanctions laws regarding Cuba as well. This means that these subsidiaries are banned by U.S. law from doing business that is completely legal under the laws of their country of organization. The United States does not, however, apply any secondary sanctions with respect to Cuba.

Asset freeze: In the past, all assets belonging to the Cuban government and to any Cuban national or entity, wherever located (except in the United States itself) were blocked. This no longer applies to Cuban nationals who are located in the United States, or who have taken up permanent residence outside of Cuba and can prove this through documentation. This exception does not apply, though, to prohibited officials of the Cuban government or the Cuban Communist Party. In addition, assets belonging to entities are unblocked if they were blocked solely because they were owned by a Cuban national whose assets have also been unblocked.

Exports: Exports of U.S. origin products and exports from the United States to Cuba are prohibited without a license. Such a license can cover only exports of U.S. origin goods or services. There are exceptions for informational materials, for donations of food, and for agricultural products. The exception for agricultural commodities applies only to specified products. Although they do not require a license per se, these exports must be reported to BIS in advance, and BIS can refuse to allow the exportation. In addition, agricultural exports can be sold only for cash in advance or with financing by a financial institution outside the United States or Cuba.

Imports: All imports from Cuba are prohibited without a license. There is an exception for imports of goods and services produced by independent Cuban entrepreneurs who have been designated as such by the State Department.

Financial transactions: Financial transactions involving a Cuban element are prohibited unless performed in connection with a licensed transaction. In a recent change, U.S. banks are prohibited from processing transactions involving a Cuban element, even if none of the other parties to the transaction is a U.S. person. There are limited exceptions to this rule, including financial transactions involving

- Remittances from "persons subject to U.S. jurisdiction" to Cuban nationals who are close relatives
- Remittances from Cuban nationals to persons subject to U.S. jurisdiction
- Cuban official missions in the United States

- Official business of the U.S. government, other foreign governments, and certain intergovernmental agencies
- Operating expenses or other official business in Cuba of third-country official missions or any intergovernmental organization in which the United States is a member

Travel: Travel by U.S. persons to Cuba is banned unless the travel falls under one of several specific categories provided for under a general license, or unless a specific license is issued. Normal "tourism" as such is not allowed without a specific license.

Banking: Despite the general embargo on trade and financial transactions with Cuba, some banking relationships with Cuba are allowed. U.S. banks can open correspondent accounts for Cuban banks. They can also process payments on credit and debit cards for travel expenses incurred during authorized travel to Cuba.

Shipping: U.S. ships are not allowed to call on Cuban ports, and Cuban ships cannot enter U.S. waters. Third-country ships that call on Cuban ports are banned from loading or unloading cargo in the United States for 180 days after the date of departure from Cuba.

Claims against Third Parties: At the time of the Cuban Revolution, the new government seized a great deal of property belonging to persons who had fled Cuba. Some of this property may have subsequently been sold to third parties outside of Cuba. U.S. law allows for the owners of such property to sue these buyers, as well as others who use property seized by the Cuban government. The United States had long suspended this right, but it was reinstated in 2019. The first suit filed was against Carnival Cruise Lines, which docks at property in Havana that a U.S. citizen claims was expropriated from his family.

Other exceptions: Mail and telecommunications between the United States and Cuba are allowed, as are transactions involving information and informational materials.

Cyber-Related Sanctions

This sanctions program authorizes the President to designate as SDNs any persons or entities engaged in cyber-related activities outside the United States that threaten the national security or economy of the country.

Democratic Republic of the Congo-Related Sanctions

Various individuals and groups in the DRC have been designated as SDNs for committing violence and undermining peace and security in the DRC.

Foreign Interference in a United States Election Sanctions

This program was instituted in response to a finding of attempts by Russia to interfere in the 2016 U.S. Presidential election. Under this program, the President can apply a range of sanctions to individuals and entities ("persons") found to have interfered in U.S. elections, including:

- blocking and prohibiting all transactions in a person's property and interests in property subject to United States jurisdiction;
- imposing export license restrictions;
- prohibiting U.S. financial institutions making loans or providing credit to the person;
- imposing restrictions on transactions in foreign exchange in which a person has any interest;
- prohibiting transfers of credit or payments between financial institutions, or by, through, or to any financial institution, for the benefit of a person;
- prohibiting U.S. persons from investing in or purchasing equity or debt of a person;
- excluding an entity's alien corporate officers from the United States;
- imposing on a person's alien principal executive officers of any of the sanctions described in this section; or
- any other measures authorized by law.

Global Magnitsky Sanctions

These sanctions authorize the designation as SDNs of persons anywhere in the world who commit serious human rights abuses or who engage in corruption.

OFAC Web Site:

https://www.treasury.gov/resource-center/sanctions/Programs/pages/glomag.aspx

Iran Sanctions

The U.S. sanctions against Iran are possibly the single most extensive and complicated sanctions program in the world. Although this program institutes a general embargo on trade with Iran, there are a number of exceptions. Importantly, this program also allows for the imposition of secondary sanctions – sanctions on persons who engage in certain types of transactions involving Iran. An indication of the complexity of the Iran sanctions is that there are four separate sets of sanctions regulations and 24 separate Executive Orders imposing sanctions on Iran. The main sets of regulations are the Iranian Transactions and Sanctions Regulations, which cover transactions by U.S. and some non-U.S. persons, and the Iranian Financial Sanctions Regulations, which apply primarily to non-U.S. financial institutions.

Coverage: The Iran sanctions apply to U.S. persons. In addition, under §560.215 of the ITSR:

> an entity that is owned or controlled by a United States person and established or maintained outside the United States is prohibited from knowingly engaging in any transaction, directly or indirectly, with the Government of Iran or any person subject to the jurisdiction of the Government of Iran that would be prohibited pursuant to this part if engaged in by a United States person or in the United States.

This means that, effectively, the U.S. sanctions against Iran apply to the foreign subsidiaries of U.S. companies. However, the regulation also imposes a control test, so that if a foreign entity is controlled by a U.S. person, the prohibition also applies. In this case, “control” is defined very broadly. The conduct must be knowing, but it is unclear whether this would provide much protection. Conversely, foreign subsidiaries are allowed to engage in transactions to the extent that their U.S. owners could, so that they may also do business with Iran if the business is covered by an exception or general license.

The Iran sanctions may also apply to non-U.S. persons. As discussed below, if a non-U.S. person engages in certain types of conduct, the United States may impose penalties on it. These types of conduct include providing material support for certain designated activities or knowingly engaging in significant transactions.

Iranian sanctions apply to the territory of Iran and the Iranian government. They do not apply to Iranian nationals who can prove that they reside outside Iran.

Asset freeze: The United States has designated major Iranian officials, including the Supreme Leader and the Minister of Foreign Affairs, as SDNs. The United States has also designated major components of the Iranian government, most notably the Iranian Revolutionary Guard Corps (IRGC), as SDNs. The designation of the IRGC as an SDN is especially notable because the IRGC owns or controls a substantial portion of the Iranian economy. As a consequence of OFAC’s 50 percent rule, all entities owned by the IRGC are also considered to be SDNs, even if they have not been separately designated. All of the major Iranian banks have been designated as SDNs, so that any meaningful commercial transaction with Iran is likely to involve an SDN. Finally, OFAC has designated hundreds of Iranian companies, organizations, and individuals as SDNs. Collectively, SDNs account for a sizable share of all Iranian economic activity. These include the National Iranian Oil Company (NIOC) and the Islamic Republic of Iran Shipping Line (IRISL).

Exports: Exports of U.S. origin goods, services, and technology and exports of these items from the United States to Iran are prohibited without a license. This prohibition includes a ban on credit or loans to Iran.

The re-exportation of U.S. goods from third countries to Iran is prohibited if the seller knew or had reason to know that the products would be re-exported to Iran.

Such re-exports are also prohibited if (1) the buyer is not a U.S. person, (2) the buyer knew or had reason to know that the products were intended for Iran, and (3) the products are subject to U.S. export licensing requirements (i.e., they are not classified as EAR 99, products which do not require a license for export). In addition, the re-export of products made in a third country that contain 10 percent or more U.S. content, by value, also require a license if the U.S. content (whether in the form of goods, services, or technology) was subject to export control requirements.

There are exceptions to the export licensing requirement for informational materials, for humanitarian donations, and for agricultural and medical products. The exception for agricultural commodities and medical products takes the form of a general license, and applies only to specified products. The general license authorizes practically all activities associated with such exports, including "the making of shipping and cargo inspection arrangements, the obtaining of insurance, the arrangement of financing and payment, shipping of the goods, receipt of payment, and the entry into contracts (including executory contracts)." Unlike the situation with Cuba, there is no duty to inform OFAC or the Commerce Department, but transactions must be completed within 12 months of the signing of the contract. Significantly, this general license authorizes sales to the Government of Iran and to any person or entity in Iran, except, in the case of agricultural commodities, to military, intelligence, or law enforcement purchasers. The regulation also restricts the terms of payment, allowing cash in advance, sales on open account (but only if credit is provided by the seller), financing by a third country financial institution, or a letter of credit issued by certain Iranian banks.

Exports of civil aircraft, parts, and related services to Iran require a specific license. Such exports were formerly subject to a favorable licensing policy, but this policy was revoked in 2018 as part of the Trump Administration's general tightening of sanctions against Iran.

Imports: All imports from Iran are prohibited without a license. The only exceptions are for gifts and for informational materials already in existence.

Investment: U.S. persons cannot make any investment in Iran, or in entities owned or controlled by the Iranian government.

Financial transactions: Financial transactions involving a Iranian element are prohibited unless performed in connection with a licensed transaction or a transaction falling under an exception to the Iran sanctions. There are limited exceptions to this rule, including financial transactions involving

- Iranian government missions in the United States
- payments for overflights of Iranian airspace
- operating expenses of third country diplomatic and consular missions in Iran

- the sale of real or personal property located in Iran that belong to a U.S. person
- living expenses of U.S. persons residing in Iran

Travel: Travel by U.S. persons to Iran is allowed. Payment of ordinary travel expenses while traveling in Iran is also allowed.

Other exceptions: Mail and telecommunications between the United States and Iran are allowed, as are transactions involving information and informational materials.

Secondary sanctions: In addition to the above sanctions, which apply to U.S. persons (and foreign entities owned or controlled by them), the United States imposes a range of so-called secondary sanctions. These are sanctions directed at non-U.S. persons for engaging in certain types of activities. In general, the United States may impose sanctions if a non-U.S. person provides material support for, or engages in significant transactions involving, the following sectors of the Iranian economy:

- Energy
- Petroleum and petroleum products
- Shipping
- Shipbuilding
- Automotive production
- Iron, steel, aluminum, or copper

The United States may also impose secondary sanctions if a foreign person deals with a range of Iranian SDNs, including the IRGC. The sanctions that can be imposed under secondary sanctions range from the "menu sanctions" described above to mandatory designation as an SDN. Foreign financial institutions that engage in certain proscribed transactions regarding Iran can be denied correspondent or pass-through accounts at U.S. banks, essentially denying them direct access to the U.S. financial system.

In most cases, the application of secondary sanctions requires that the foreign person either provide material support or engage in a "significant" transaction. OFAC has not defined "material support." In assessing whether a transaction is significant, OFAC will consider the following factors:

1. the size, number, and frequency of the transaction(s);
2. the nature of the transaction(s);
3. the level of awareness of management and whether the transaction(s) are part of a pattern of conduct;
4. the nexus between the transaction(s) and a blocked person; (
5. the impact of the transaction(s) on statutory objectives;
6. whether the transaction(s) involve deceptive practices; and
7. any other relevant factors

Iraq-Related Sanctions

Lebanon-Related Sanctions

Libya Sanctions

The United States formerly had broad sanctions against Libya in place. These were mostly removed falling the fall of Qadafi. Current sanctions primarily take the form of the designation as SDNs of persons undermining peace and stability in Libya, and misappropriating state assets.

Magnitsky Sanctions

Mali-Related Sanctions

Nicaragua-Related Sanctions

Non-Proliferation Sanctions

North Korea Sanctions

In line with the UN sanctions, the United States has imposed comprehensive sanctions against North Korea. Indeed, North Korea may be subject to the most extensive set of sanctions of any country.

Coverage: The U.S. sanctions against North Korea apply to all U.S. persons. In addition, non-U.S. persons who engage in certain types of transactions may be subject to secondary sanctions, as discussed below.

Asset freeze: The United States has essentially designated the entire country of North Korea as an SDN. U.S. persons are required to block any assets belonging to the North Korean government and the Workers' Party of North Korea. In addition, OFAC can designate as an SDN any person or entity it finds to be "a North Korea person." While not every person and company in North Korea has been designated as an SDN, this authority potentially reaches the assets of any North Korean individual or entity worldwide. The United States may also impose an asset freeze on persons doing certain types of business with North Korea, as discussed below.

Imports and exports: U.S. law prohibits basically all imports from and exports (including re-exports) to North Korea. "Exports" includes financial services, so basically no U.S. bank can handle any transaction with a North Korean .

Investment: U.S. investment in North Korea is prohibited.

Travel: Travel by U.S. persons to North Korea is prohibited.

- **Exceptions**: There are limited exceptions to the embargo against North Korea, including
- The provision of certain legal services to North Korean persons
- The payment of legal fees by North Korean persons from funds located outside of North Korea
- Transactions involving the North Korean mission to the United Nations
- Non-commercial personal remittances
- Official business of the U.S. federal government
- Third-country diplomatic and consular funds transfers
- Telecommunications and mail

Secondary sanctions: The United States may designate as SDNs person who, among other activities:

- Export arms, or support the export of arms, to North Korea
- Export luxury goods to North Korea
- Sell or purchase, directly or indirectly, to or from North Korea metal, graphite, coal, or software
- Engage in, facilitate, or are responsible for the exportation of workers from North Korea
- Operate in the construction, energy, financial services, fishing, information technology, manufacturing, medical, mining, textiles, or transportation industries in North Korea
- Have engaged in at least one significant importation from or exportation to North Korea of any goods, services, or technology
- Have knowingly conducted or facilitated any significant transaction with a North Korean SDN or in connection with trade with North Korea.

Under these sanctions, the United States could designate as an SDN a party for performing even a single transaction with North Korea, if the transaction was considered significant. Non-U.S. persons operating joint ventures in North Korea in a number of major industries and sectors are also subject to designation.

In addition, foreign financial institutions that perform any significant transactions with North Korea, including trade with North Korea, may be prohibited from opening or maintaining correspondent or payable-through accounts in the United States, or subjected to strict conditions for the operation of such accounts.

Rough Diamond Trade Controls

The United States prohibits the importation of rough diamonds from countries that are not parties to the Kimberley Process Certification Scheme, which ensures that diamonds are produced from reputable source, and are not used to support organizations engaging in violence or human rights violations.

Somalia Sanctions

The main sanctions under the Somalia program involve the designation as SDNs of various persons and entities undermining peace and stability in Somalia. The United States has also implemented the UN ban on the importation of charcoal from Somalia.

Sudan and Darfur Sanctions

The United States formerly had broad based sanctions against Sudan that prohibited most transactions with that country. These sanctions were mostly lifted in 2017. The present sanctions designate as SDNs, and block the property of, various individuals and organizations engaged in the suppression of democracy and the violation of human rights, especially in Darfur. Although OFAC's web site still refers to Sudan sanctions, the only sanctions program actually in effect is directed towards violence in the Darfur region of Sudan.

South Sudan-Related Sanctions

Syria Sanctions

The United States has imposed broad sanctions against Syria that effectively prohibit almost all transactions.

Asset freezes: The United States has blocked all assets belonging to the Syrian government, so that any U.S. person must freeze property belonging to the Government of Syria over which they gain possession or control. The United States has also designated as SDNs a variety of government leaders and organizations, as well as commercial companies within Syria. Probably the most important of these is the Commercial Bank of Syria, the largest bank in the country. This designation makes it difficult or impossible as a practical matter for U.S. persons to conduct any transactions with Syria. Many Syrian entities, including the Commercial Bank of Syria, have been designated under OFAC programs other than the Syria program; the Commercial Bank of Syria, for example, was designated as an SDN under the Non-Proliferation Weapons of Mass Destruction program.

Exports: OFAC regulations prohibit the exportation of any services to Syria. Exports of U.S. goods to Syria are not prohibited as such, but all exports other than designated food or medicine require a license from BIS. BIS's Syria licensing policy is one of denial.

Imports: Imports of petroleum products of Syrian origin into the United States are prohibited. In fact, U.S. persons may not engage in transactions involving the purchase, sale, or transportation of petroleum and petroleum products of Syrian origin, even if the products are not destined for importation into the United States. Because the Commercial Bank of Syria and a number of other Syrian banks have been designated as SDNs, though, any sort of commercial transaction with Syria by U.S. persons is difficult.

Investment: U.S. investment in Syria is prohibited.

Exceptions: There are a number of exceptions to the Syria sanctions, including

- Exports of designated food and medical products from the United States to Syria
- Non-commercial personal remittances to or from Syria
- Transactions involving U.S. persons resident in Syria
- The export of goods and services in support of humanitarian activities in Syria
- Telecommunications and mail
- Transactions involving Syrian diplomatic missions in the United States
- Third-country diplomatic and consular funds transfers

Secondary Sanctions: The United States may designate as SDNs individuals or entities providing material support to the Syrian government. The United States has designated a number of Russian banks under this provision. Under CAATSA, the United States may also impose sanctions on non-U.S. persons exporting, or supporting the exportation, of arms and related materiel to Syria.

Transnational Criminal Organizations

Ukraine-/Russia-Related Sanctions

The United States has imposed sanctions against various Russian and Ukrainian individuals and entities in connection with Russia's activities in Eastern Ukraine and its annexation of Crimea. Although the sanctions are directed at Russia's actions in Ukraine, the sanctions apply mainly to Russian rather than Ukrainian persons. These are not the only U.S. sanctions directed primarily at Russian persons; the CAATSA, Cyber-Related, Electoral Interference, and Magnitsky programs are also focused primarily on Russian persons. Despite the complexity of the Russia sanctions, most transactions between the United States and Russia are still allowed.

Asset freeze: The United States has designated as SDNs a number of Russian individuals and entities. These include various Russian officials and, significantly, a number of so-called oligarchs. These designations are significant because, unlike most SDNs, these oligarchs and their holdings (which are also designated under the OFAC 50% rule) include major companies that are fully integrated into the global economy.

Crimea: In response to the Russian annexation of Crimea, the United States has prohibited all imports from, and all exports to, the Crimea region of Ukraine, as well as any new investment in Crimea. A number of major entities in Crimea have also been designated as SDNs.

Imports: The United States does not prohibit imports from Russia, although imports of certain weapons and other arms are effectively banned, as their Russian manufacturers have been designated as SDNs.

Exports: Most exports to Russia are allowed. Items on the Munitions List and items subject to export controls as dual-use goods for national security reasons, however. In addition, certain exports of goods, services, and technology subject to Directive 4 are prohibited, as discussed below in the section on Sectoral Sanctions.

Investment: There are no restrictions on U.S. investment in Russia. OFAC has held that a U.S. company violates the law, though, if it signs a contract where the signatory for the Russian partner is an SDN, even though the Russian company itself has not been designated and even though the SDN does not meet the 50% ownership test.

Banking and financial transactions: U.S. persons are prohibited from dealing in certain debt and equity of designated Russian entities under Directives 1, 2, and 3, as discussed below in the section on sectoral sanctions. U.S. banks are prohibited from acting in the primary market for sovereign Russian debt, and from making non-ruble denominated loans to the Russian government. In this context, "sovereign" means "any ministry, agency, or sovereign fund of the Russian Federation, including the Central Bank of Russia, the National Wealth Fund, and the Ministry of Finance of the Russian Federation." However, this ban does not apply to loans to state-owned enterprises in Russia. Otherwise, all financial transactions with Russia and with Russian entities, including making loans, purchasing equity, and processing payments, are allowed.

Sectoral sanctions: Russia is uniquely subject to sectoral sanctions. These are fairly narrowly-targeted sanctions, similar to those imposed by the European Union, that prohibit only certain types of transactions with designated companies. The U.S. sectoral sanctions are set forth in four directives.

Directive 1 prohibits U.S. persons from dealing in equity of designated Russian banks issued after a fixed date. It also prohibits U.S. persons from dealing in debt of these same Russian persons with a maturity of greater than 14 days, again issued after a date identified in the Directive. The effect of this directive is to limit the ability of U.S. banks and other U.S. persons to provide anything other than short-term loans to the designated Russian banks. In addition, U.S. persons cannot buy, sell, trade, or indeed be involved in any transactions regarding bonds and other debt of these Russian banks with a maturity longer than 14 days. All other transactions with these Russian banks, including the processing of payments, are permitted. Directive 1 only applies to the debt of the banks themselves, not their customers. Nor does Directive 1 prevent U.S. persons from obtaining loans from Russian banks.

Directive 2 is similar to Directive 1, but applies to the debt of designated energy companies with a maturity of more than 60 days. Directive 2 does not apply to equity, so that U.S. persons are free to buy and sell shares in the firms subject to Directive 2, such as Gazprom.

Directive 3 prohibits U.S. persons from dealing in debt with a maturity of longer than 30 days of designated companies in the Russian defense sector.

Directive 4 prohibits the export of goods, services, or technology from the United States to certain designated Russian energy companies where the item is to be used in support of the exploration for or production of petroleum from deepwater, Arctic offshore, or shale projects in the Russian Federation. The same prohibition applies to any projects anywhere in the world that were initiated on or after January 29, 2018 and in which a Russian person designated under Directive 4 has an ownership interest of at least 33 percent, or ownership of a majority of voting interests.

Secondary sanctions: The United States may impose secondary sanctions against foreign persons engaging in certain transactions, including

- Any transaction with an SDN in the Russian Federation
- Transactions with persons designated as belonging to the intelligence and defense sectors of the Russian Federation
- Development of energy pipelines in Russia
- Participation in the privatization of state-owned assets in Russia
- Assistance in evading sanctions against Russia.

The penalties imposed may include designation as an SDN, as well as the other “menu” sanctions described above.

Venezuela-Related Sanctions

The United States has imposed increasingly strict sanctions against Venezuela in response to the Maduro regime’s actions. While most transactions between Venezuela and the United States theoretically remain legal, the blocking of all assets belonging to the Venezuelan government, including all state-owned companies, has greatly restricted U.S. trade with Venezuela.

Asset freeze: The United States has blocked all assets belonging to the Venezuelan government. This includes the Venezuelan state-owned oil company, Petroleos de Venezuela S.A. (PdVSA). This means that U.S. persons cannot participate in any transaction involving the Venezuelan government or PdVSA, as well as other state-owned companies. An Executive Order also authorizes OFAC to designate as SDNs anyone active in the gold sector in Venezuela, as well as those committing or concealing corruption.

Imports: There are no restrictions on imports from Venezuela as such. In particular, it is legal to import Venezuelan oil into the United States. However, the main source of Venezuelan oil is PdVSA, which is blocked. As a practical matter this means that Venezuelan oil can be imported only if a license applies.

Exports: There are no sanctions restrictions on exports to Venezuela, although other export control laws apply.

Banking and finance: In general, most banking transactions with Venezuela are allowed. However, U.S. sanctions prohibit certain types of transactions involving the debt or assets of the Venezuelan government, including

- the purchase of any debt owed to the Government of Venezuela, including accounts receivable;
- any debt owed to the Government of Venezuela that is pledged as collateral, including accounts receivable; and
- the sale, transfer, assignment, or pledging as collateral by the Government of Venezuela of any equity interest in any entity in which the Government of Venezuela has a 50 percent or greater ownership interest.

Exceptions: There are currently 34 general licenses applying to Venezuela. Among other things, these allow certain transactions with PdVSA; authorize U.S. persons to wind down contracts with the Venezuelan government and Venezuelan state-owned entities; and exempt CITGO, a U.S. oil company owned by the Government of Venezuela, from the blocking of Venezuelan government assets so that it can continue in business.

Yemen-Related Sanctions

Zimbabwe Sanctions

Compliance

Compliance with U.S. sanctions is of course mandatory for U.S. persons. It may also be necessary for non-U.S. persons to avoid secondary sanctions. OFAC does not, however, impose any specific requirements for sanctions compliance systems. Rather, OFAC states that companies

should develop a tailored, risk-based compliance program, which may include sanctions list screening or other appropriate measures. An adequate compliance solution will depend on a variety of factors, including the type of business involved, and there is no single compliance program or solution suitable for every circumstance.

Although it does not impose any requirements regarding a sanctions compliance system, OFAC has issued "A Framework for OFAC Compliance Commitments." A link to this document is included in the reference materials in the Appendix. These guidelines largely mirror the EU guidance. OFAC identifies the main components of a sanctions compliance system as including:

1. Management commitment to sanctions compliance;
2. A risk assessment identifying the entity's sanctions risks;
3. A system of internal controls that mitigate the identified risks;
4. Procedures for testing and auditing the functioning of the system; and
5. Training regarding both substantive sanctions requirements and the operation of the sanctions compliance system.

Each of these elements will be discussed in detail in Section 5 regarding compliance systems.

While the lack of concrete requirements leaves companies and other organizations the flexibility to design their own systems for complying with sanctions, it also means that, in case of a violation of sanctions laws, there is no way a company can demonstrate that it has "an adequate compliance solution." As discussed below, the United States government applies an effective strict liability regime to sanctions; if there is a violation, the party committing the violation can be held liable. There are no safe harbors. However, OFAC will consider the design and implementation of a compliance system in deciding what if any penalty to impose in case of sanctions violations. The presence of a well-designed system that complies with OFAC guidelines and industry best practices could result in substantially reduced penalties.

U.S. persons are subject to certain reporting and record-keeping requirements. Anyone who blocks (i.e., freezes) property is required to file a report with OFAC within 10 days. The same is true of persons, primarily banks, who reject transactions that cannot be performed, but where blocking is not required, as with many transactions involving Iran. These reports must be filed within 10 days as well. U.S. persons are required to keep records of all transaction subject to sanctions, including those authorized by licenses or subject to an exemption from the sanctions laws, for five years. The same requirement applies for those holding blocked property.

Enforcement

U.S. persons, and in some cases non-U.S. persons, are responsible for complying with U.S. sanctions laws. Sanctions enforcement in the United States occurs mostly at the federal level, but New York state in particular may also be involved.

Primary enforcement is by OFAC. The Department of Justice may be involved, though, if a case is sufficiently serious. The Bureau of Industry and Security is the primary enforcer of the U.S. export control laws. Because of the interaction between sanctions and export control laws, it may work with OFAC in some cases. FinCen, the U.S. financial intelligence agency, which is also located with the Treasury Department, is primarily responsible for enforcing the anti-money laundering laws, but much of its guidance is applicable to sanctions as well, and it publishes important advisories on sanctions topics.

Banks are subject to their own regulatory regime. While the primary bank regulator at the federal level in the United States is the Office of the Comptroller of the Currency, the Federal Reserve is also involved, especially in sanctions cases. Finally, for banks with a New York presence, the New York Department of Financial Services has been very active in investigating banks where it deemed sanctions violations were also violations of New York's business records laws.

A full discussion of the enforcement procedure in the United States appears in Section 7, "Enforcement," below.

Russia

In accordance with Federal Law No. 281-FZ dated 22 December 2006 On Special Economic Measures, Russia implements UN sanctions with presidential decrees.

Resolution of the Government of the Russian Federation No 778 dated 7 August 2014 (as amended) have imposed a ban on import of certain listed agricultural products, raw materials, foodstuffs from the United States of America, the European Union countries, Canada, Australia, Norway, Ukraine, Albania, Montenegro, Iceland, Liechtenstein. In addition Russia has introduced also travel bans against certain EU, American and Canadian politicians and military leaders from entering to Russia.

The Federal Financial Monitoring Services has a list of entities and individuals against whom there is evidence of participating in extremist activities or terrorism. The list can be found at http://fedsfm.ru/documents/terr-list.

Other Players in the International Arena

Financial Action Task Force

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. Members are currently 37 jurisdictions and 2 regional organizations, representing most major financial centers in all parts of the globe.

The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.

The FATF does not impose sanctions, but is a “policy-making body” which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas. This includes financial sanctions.

The FATF has developed a series of Recommendations that are recognised as the international standard for combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. They form the basis for a co-ordinated response to these threats to the integrity of the financial system and help ensure a level playing field.

The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally. In collaboration with other international stakeholders, the FATF works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

The FATF document “International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation” (the FATF Recommendations) includes a few recommendations related to financial sanctions:

Recommendation 6: Targeted financial sanctions related to terrorism and terrorist financing

Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001).

Recommendation 7: Targeted financial sanctions related to proliferation

Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.

In June 2013, the FATF issued a 19-page document "International Best Practices – Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6).

The paper seeks to assist countries in developing and implementing targeted financial sanctions to prevent and suppress terrorist financing in accordance with the relevant UNSCRs and in a manner consistent with these fundamental principles, through a robust and transparent targeted financial sanctions regime.

The paper sets out non-binding guidance based on updates in relevant UNSCRs and in response to challenges faced by countries in the implementation of the requirements of Recommendation 6.

Recommendation 6 requires each country to implement the targeted financial sanctions regimes to comply with the United Nations Security Council resolutions (UNSCRs or resolutions) relating to the prevention and suppression of terrorism and terrorist financing, including:

- UNSCR 1267(1999) and its successor resolutions (the Al-Qaida/Taliban sanctions regimes);
- UNSCR 1373(2001); and
- any other UNSCRs which impose targeted financial sanctions in the terrorist financing context.

These resolutions require countries to freeze, without delay, the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council (the Security Council) under Chapter VII of the Charter of the United Nations, including in accordance with the Al-Qaida/Taliban sanctions regimes4; or (ii) designated by that country or by a supra-national jurisdiction pursuant to UNSCR 1373.

Such measures may be either judicial or administrative in nature The paper explains that the required elements of a targeted financial sanctions regime are identified in Recommendation 6 and its Interpretive Note (INR6).

The paper further explains that efforts to combat terrorist financing are greatly undermined if countries do not freeze the funds or other assets of designated persons and entities quickly and effectively. Nevertheless, in determining the limits of or fostering widespread support for an effective counter-terrorist financing regime, countries must respect human rights, respect the rule of law, allow due process, recognize and protect the rights of bona fide third parties.

The paper stresses the importance of an effective freezing regime and has four sections:

1. Clear authorities and procedures for identifying and designating persons or entities
2. Due process: review, delisting and unfreezing
3. Post designation issues: freezing and prohibiting dealing in funds or other assets of designated persons and entities
4. Designated persons and entities: Compliance and access to frozen funds or other assets

Interpol

The International Criminal Police Organization (Interpol) is an inter-governmental organization. It has 194 member countries, and it helps police in all of them to work together. Interpol enables the police forces in these countries to share and access data on crimes and criminals, and offers a range of technical and operational support.

Interpol does not issue sanctions but it has formal procedures for cooperation with United Nations Sanctions Committees and issues so called "Special Notices" for individuals and entities subject to these sanctions regimes.

Two of the UN Sanctions Committees most active in this regard are:

- The Sanctions Committee pursuant to resolutions 1267 (1999) and 1989 (2011): this Committee oversees sanctions concerning individuals and entities associated with ISIL (Daesh) and Al-Qaida.
- The Sanctions Committee pursuant to resolution 1988 (2011): this Committee oversees sanctions concerning individuals and entities associated with the Taliban;

The success of the Special Notice with these two committees has resulted in INTERPOL's cooperation being extended to other Sanctions Committees, including those concerning the Democratic Republic of Congo, Somalia, Sudan, Guinea-Bissau, the Central African Republic, Yemen, South Sudan and Libya.

The “INTERPOL-United Nations Security Council Special Notice” combines the UN sanctions regime with INTERPOL’s well-established notice system into an effective law enforcement tool.

Source image: https://www.interpol.int/en/How-we-work/Notices/About-Notices

Special Notices are issued for individuals and entities that are subject to sanctions imposed by the UNSC. Its principal function is to alert national law enforcement authorities that at least one of these forms of sanctions apply:

- Assets freeze: freezing funds or other assets. There is no requirement to seize or confiscate assets;
- Travel ban: preventing an individual from entering or transiting through territories. There is no requirement to arrest or prosecute these individuals;
- Arms embargo: preventing the direct or indirect supply, sale or transfer of arms and related materials.

Special Notices contain information that identifies the individual or entity, and explains the relevant sanctions; this assists law enforcement officers to take appropriate action in accordance with their national laws.

Since December 2017, UN Member States are encouraged to submit photographs and other biometric data of individuals for inclusion in these Special Notices under UNSC Resolution 2399.

Special Notices are circulated to all INTERPOL member countries through Interpol’s secure global communications system, and extracts of them are published on the Interpol website. More than 700 Special Notices have been issued since its creation in 2005.

Summary

- Sanctions are imposed primarily by countries, but may be imposed by international organizations as well.
- The United Nations imposes sanctions on a number of countries, individuals, and entities.
- The UN does not enforce sanctions directly; rather, they must be implemented and enforced by UN member states.
- Sanctions in the EU are imposed at both the Union and the national level.
- The European Union generally uses targeted sanctions that are focused on specific individuals and entities, so avoiding harm to "innocent bystanders."
- The EU does impose fairly broad sanctions against North Korea and Syria, though.
- The EU system has strong legal protections for sanctions targets.
- Actual enforcement of EU sanctions is by the Member States.
- The United States has the largest and most complicated system of sanctions in the world.
- Like the European Union, most U.S. sanctions are focused on individuals, entities, and organizations, including terrorists, drug dealers, weapons proliferators, and those undermining democracy and violating human rights.
- The United States imposes comprehensive sanctions against Crimea, Cuba, Iran, North Korea, and Syria. It imposes broad but less comprehensive sanctions against Russia and Venezuela.
- The FATF does not impose sanctions, but is a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in financial crime areas, including financial sanctions.

Review Questions

1. What entity within the United Nations imposes sanctions?
2. What is the underlying EU philosophy regarding the use of sanctions?
3. What agency within the EU is responsible for sanctions enforcement?
4. Against which countries has the United States imposed broad sanctions?
5. What is an SDN?
6. Describe the two Recommendations of the FATF that cover financial sanctions.
7. What are "Special Notices"?

SANCTIONS EVASION: TYPOLOGIES AND SCHEMES

Association of Certified Sanctions Specialists (ACSS)
7950 NW 53rd Street Suite 337
Miami, FL 33166
Phone: +1 305 433 7187
helpdesk@sanctionsassociation.org
www.sanctionsassociation.org

Introduction

Despite robust U.S. and United Nations (UN) sanctions on North Korea, North Korea continues to evade sanctions ….

Updated Guidance on Addressing North Korea's Illicit Shipping Practices (2019)

Sanctions can significantly isolate designated countries, companies, organizations, and persons from the global economy. In order to gain access to resources and to continue to do business, sanctions targets will try to find ways to evade sanctions. At the same time, there are individuals and companies who would like to do business with them, but who are prevented from doing so by the sanctions laws of their own or other countries. Both sets of evaders may use any of a number of tactics to escape sanctions.

Firms that engage in sanctions-busting transactions are making trade offs between profiting from the premiums created by sanctions versus the risks of potential detection and punishment.

Below is an article from www.sanctionsassociation.org that explains this.

'Sanctions Busting': The Risks and Rewards to those Trying to Circumvent the System

June 15, 2018
By: Keith Preble and Dr. Bryan R. Early

The main goal of imposing sanctions on a target country or entity has always been to disrupt the target's commercial relationships and make it costlier for them to do business. Governments try to achieve this goal by imposing administrative and criminal penalties for individuals and entities that violate their sanctions.

Though these restrictions generally apply only to firms and citizens operating in the country imposing the sanctions, the United States has recently employed far more aggressive and wide-reaching methods in penalizing foreign firms.

This has included imposing "secondary" sanctions, which target U.S. persons anywhere in the world, or "sectoral sanctions", which black-list individuals and entities for certain types of transactions Governments that adopt sanctions have significant incentives to prevent firms in both their own and foreign countries from undercutting their sanctions, as such activities dramatically reduce the likelihood of the sanctioning efforts succeeding.

As sanctions disrupt commercial relationships, affected firms must either heed the law and find new business partners or find other ways of circumventing sanctions restrictions to continue trading with their old partners.

What is 'Sanctions Busting'?

Commercial-based 'sanctions busting' occurs when sanctioned entities circumvent sanctions restrictions by finding replacement business partners or devising methods of maintaining existing relationships despite the sanctions. These strategies allow sanctioned entities to minimize the disruption and hardships that sanctions would otherwise impose, which undercuts the impact of the sanctions.

Sanctioned entities rely on businesses in states imposing sanctions or third-party states not participating in the sanctions that are willing to still do business with them despite the risks of penalties or potential reputational costs.

Direct Violation and Legal Loopholes

Though penalties remain high, especially in the United States, doing business with sanctioned entities can still be lucrative, depending upon how badly the sanctions have affected their targets' terms of trade. It can be very profitable for businesses in third-party states or in the sanctioner state(s) willing to tolerate the risks of detection and punishment, and to 'sanctions-bust' on behalf of targeted entities.

Some sanctions-busting commerce will directly violate the sender governments' laws while other forms can exploit legal loopholes or are not explicitly forbidden. Variation in the jurisdictional scope of sanctions will influence the degree to which firms face potential legal punishments as opposed to ad hoc retaliation for undercutting sanctions.

Some sanctions policies can leave loopholes that allow foreign-owned subsidiaries to continue doing business with sanctioned parties. For example, it wasn't until the passage of the Iran Threat Reduction and Syria Human Rights Act of 2012 that U.S. firms became liable for their foreign-owned subsidiaries' violations of U.S. sanctions policies vis-à-vis Iran.

Business Relocation

Firms and even governments can go to elaborate lengths to engage in sanctions busting. One of the most straightforward methods is for firms to relocate their business to third-party states that are not participating in the sanctions. This can be done by employing brokers or "middle-men" to facilitate transactions as intermediaries in third-party states.

Alternatively, firms from sanctions-imposing states can set up their own operations in third-party venues. In the case of the U.S.-led sanctions against Iran, for example, Dubai in the United Arab Emirates emerged as a critical intermediary for trading to and from Iran for many years.

Obscuring Transactions

Not surprisingly, the fear of possible detection and punishment by sender governments will give firms a strong incentive to hide their sanctions-busting transactions. To that end, they may develop strategies for obscuring the point of origin or end-destination of products by employing complex transactions, front companies, illicit diversions, or smuggling tactics. They may also employ elaborately structured shell companies, fraud, money laundering, or informal financial networks to finance illicit or gray market transactions that violate sanctions. For example, numerous European banks, such as HSBC, Credit Suisse and BNP Paribas were penalized hundreds of millions of dollars by the U.S. government for facilitating transactions that violated U.S. sanctions policies.

Importance of International Cooperation

While sanctions busting often involves violating the law, a significant amount occurs openly between third-party and target states through legitimate channels when third-party governments refuse to cooperate in imposing sanctions.

The decision to cooperate with a sanctioning effort is highly political for third-party governments and takes into account the foreign policy interests and the commercial interests of their constituents. Governments cannot only refuse to join multilateral sanctioning efforts but may also push back against the use of secondary sanctions against their firms by sender governments.

The European Union (EU), for example, is seeking to protect its firms from U.S. secondary sanctions over their trade with Iran by employing blocking that would bar EU firms from complying with renewed U.S. sanctions. The EU successfully used this statute during the 1990s to protect its firms from having to comply with expansive U.S. sanctions imposed against Cuba. The benefit of such a statute is that it politicizes any secondary sanctions that would be imposed by the U.S. Government on EU firms, turning the action from a law enforcement issue into a diplomatic one. Even so, being caught in the middle of diplomatic disputes creates uncertainty and will tend to hurt their bottom lines.

Third-party governments can also use other forms of push back to protect their firms from secondary sanctions. The Chinese government lobbied the Trump Administration hard on ZTE's behalf, for example, after the U.S. government imposed harsh penalties that would have blocked its access to critical U.S. technologies and components. Formal channels also exist, in some cases, for foreign firms to request exemptions from U.S. extraterritorial sanctions obligations, and third-party governments can offer political support for those requests.

Risk vs. Reward

Firms that engage in sanctions-busting transactions are making tradeoffs between profiting from the premiums created by sanctions versus the risks of potential detection and punishment.

Sanctions-busting is driven by profits but inherently affected by politics as well. Most firms will prefer to find venues where sanctions-busting can be conducted without having to break any laws. Increasingly expansive sanctions policies adopted by the U.S., in particular, mean that many sanctions-busting transactions necessarily entail breaking at least some country's laws. This can be an effective deterrent to keep large multinational firms from sanctions-busting, especially given the U.S. Government's demonstrated willingness to impose large fines on foreign companies. At the same time, it could also encourage small and medium-sized enterprises in foreign countries to adopt strategies that increasingly rely on grey market or illicit tactics in order to hide their transactions.

For larger-sized, risk-averse businesses, and especially those that rely on doing business in the U.S. or with U.S. entities, the best option in the current business environment is to comply with their own governments' sanctions policies and to also comply with U.S. sanctions policies.

This chapter will focus on sanctions evasion in the financial and trade sectors. It will also discuss red flags that may indicate that someone is attempting to evade sanctions. It will conclude with a case study of North Korea, which is subject to comprehensive international sanctions, and which has been particularly inventive in finding ways to evade them.

Sanctions Evasion in the Financial Sector

Money moves primarily through the banking system. Most large international banks in particular have implemented sophisticated systems for reviewing information about customers and transactions to identify and stop transactions that may be subject to sanctions. To avoid these controls, individuals, companies, and countries seeking to evade sanctions have developed a range of techniques.

Stripping

Banks and other financial institutions communicate through the exchange of electronic messages. For domestic transactions, the main systems used are EPA (in Europe) and ACH (in the United States). Internationally, banks communicate through the SWIFT system. Messages are used to do everything from provide information on a transaction to direct the actual transfer of funds. Different types of messages are used for different purposes. Internationally, the two most common message types are the SWIFT MT103, which is used for cross-border transfers of funds, and the MT202 COV, which is used for funds transfers between financial institutions. A single transaction may use more than one message type; a typical international funds transfer will involve both an MT103 and MT202 COV, for example. While the information shown on each message type may vary, they generally show such basic information as the customer, the beneficiary, and the banks involved. Banks routinely screen all payment messages to identify whether any of the parties involved are (1) on an applicable sanctions list (or an internal list), or (2) located in a country subject to sanctions.

The most basic way of evading screening is simply to delete – "strip" – information from a message that would reveal the presence of a sanctioned party. "**Stripping**" is the deliberate act of deleting or changing information from payment messages or instructions. This makes it more difficult to identify payments or to connect them to sanctioned parties, individuals or countries. To counteract this, banks will typically reject transactions where fields in a message are left blank.

In some cases, some personnel in banks may wish to disguise transactions themselves, so as to fool their own screening systems, as well as those of correspondent banks. U.S. dollar transactions, for example, are almost always cleared through U.S. banks. Foreign banks that have decided that they want to do business that they knew was prohibited by U.S. sanctions, and would be stopped by their U.S. correspondent banks, have devised a variant of stripping. Rather than simply delete information, they substitute information in the relevant fields, such as by using a code word. If the name of one of the parties is on a sanctions list, for example, the relevant field in the payment message may simply say "customer" instead. Another example is the use of the bank's name instead of the customer's name in the relevant field.

Red flags: Indicators that stripping may have occurred include

- Obviously missing relevant information
- Use of placeholders, such as "customer"
- Use of the bank's own name in the customer field
- Statements such as "do not mention Iran connection"

Resubmission of Rejected Transactions

In some cases, as with the U.S. sanctions against Iran, a U.S. bank is required to reject a transaction, but not freeze the funds involved. If a bank rejects a transaction, another evasion technique is to resubmit the transaction, but after changing information in the message. This an be done by deleting the information that would tie the payment to a sanctioned party or country, or, again, but substituting new names for old. To counteract this, most banks use software that will identify resubmitted payments because the amounts or most of the parties are the same.

Red flags: A rejected payment may have been resubmitted if:

- The payment amount is identical to a rejected payment, but the names of the parties are different
- A series of payments involving the same parties total the same amount as in a rejected payment

Use of Cover Payments

For international transfers in particular, a transaction may include a "cover" payment between two banks. A Dutch bank sending funds denominated in U.S. dollars, for example, to a Mexican bank would probably route the transaction through a correspondent bank in the United States. The Dutch bank would send a "cover" payment to the U.S. bank, directing it to transfer funds from its account with the U.S. bank to an account at the Mexican bank's correspondent bank in the United States.

In the past, cover payment messages required less information than regular payment messages. Foreign banks might send a cover message to a U.S. bank that did not show the identity of all the parties involved. The U.S. bank would then routinely process a transaction that might actually be illegal under U.S. law. The mandatory use of the SWIFT MT202 COV message prevents this. Still, the use of cover messages other than the MT202 COV might be evidence of an attempt to evade sanctions.

Red flags: Evidence that a cover payment may have been used to conceal a sanctioned element include:

- Use of an MT202 message when an MT202 COV would normally be used
- Receipt of an MT202 message from a high risk customer
- Different payment instructions for U.S. dollar-denominated transactions

Use of Suspense Accounts

Banks use suspense accounts to record transactions temporarily, until the final treatment of the transaction (i.e., its allocation to customer or other accounts) can be decided. If a bank is trying to disguise a sanctioned element, it may route sanctioned transactions through a suspense account, as such transactions do not normally pass through the bank's filters.

Red flags: A bank may be misusing a suspense account to evade sanctions if

- The customer associated with the transaction is not identified
- Another financial institution is listed as the originator of the transaction

Special Purpose Entities and Front Companies

One way to disguise the role of a sanctioned party in a transaction is to route the transaction through a Special Purpose Entity (SPE). These may be shell companies – companies that have no assets or business. Sanctions evaders may also use investment funds or other types of vehicles to disguise their role in a transaction. They may also use front companies – companies that have an actual business, but where the transaction does not fit in with the company's normal lines of business

Red flags: Red flags for the use of SPEs and front companies include:

- Involvement in a transaction of a company that has no other visible business or purpose
- Parties that share an address with a number of other companies
- A company's normal business does not fit in with the transaction
- There is a pattern of large but infrequent transactions, indicating the involvement of an SPE

Layered Payments

Layering payments, which is a common means of laundering money, may also be used to evade sanctions. Layering involves using a number of different payments, possibly involving a number of different payors and beneficiaries, to perform a single transaction. The aim is to make the transaction so complicated that the screening process does not identify a sanctioned element.

Red flags: Evidence that layering may be being used to evade sanctions includes

- Complicated transactions where there is no evident need for all the different steps
- The involvement of banks and other parties without an obvious business purpose
- The transaction involves shell companies

Use of Third-Party Financial Institutions

Most normal transactions involve a limited number of financial institutions – typically, the buyer's bank and the seller's bank. If the transaction is international, and especially if it involves a currency different from those of the buyer's and seller's home countries, correspondent banks may also be involved. In a variant of layering, sanctions evaders may use third-party financial institutions to route the transaction. If a bank is trying to evade sanctions, this technique may take the form of sending a payment through a correspondent bank in a country, even if the bank has a branch in that country.

Red flags: Indicators that third-party financial institutions are being used to evade sanctions include:

- Participation of a financial institution with no apparent function
- Unexpected involvement of a correspondent bank, such as when the originating bank has a branch in the same country

- A sudden change in banking relationships, possibly connected with a sanctions event

Use of Non-Bank Financial Institutions

While most international business is conducted through banks, individuals and even businesses may use non-bank financial institutions, such as exchange houses, money service providers, and hawalas. While most such non-bank FIs are legitimate, they often have sanctions compliance systems that are less robust than those of banks, if indeed they have such a system at all. In particular, they may not conduct full customer due diligence, and may not screen transactions against sanctions lists or for the involvement of a sanctioned country. Sanctions evaders may use these non-bank FIs to gain entrée to the international financial system.

Red flags: A non-bank FI may be used for sanctions evasion if

- The non-bank FI is of a type, such as exchange houses,
- The transaction is very large
- A transaction passes through multiple exchange houses or other non-bank FIs
- The transaction is of a type that would normally pass through the regular banking system
- There are a series of transactions through a non-bank FI that seem to form a pattern that may reflect an attempt to conceal something

Virtual Currencies

The use of virtual currencies is a new phenomenon in international commerce.

OFAC offers the following definition of virtual currencies in the Frequently Asked Questions page on its website:

> FAQ 559 - For purposes of OFAC sanctions programs, what do the terms “virtual currency,” “digital currency,” “digital currency wallet,” and “digital currency address” mean?
>
> Virtual currency is a digital representation of value that functions as (i) a medium of exchange; (ii) a unit of account; and/or (iii) a store of value; is neither issued nor guaranteed by any jurisdiction; and does not have legal tender status in any jurisdiction.
>
> Digital currency includes sovereign cryptocurrency, virtual currency (non-fiat), and a digital representation of fiat currency.

A digital currency wallet is a software application (or other mechanism) that provides a means for holding, storing, and transferring digital currency.

A wallet holds the user's digital currency addresses, which allow the user to receive digital currency, and private keys, which allow the user to transfer digital currency.

The wallet also maintains the user's digital currency balance. A wallet provider is a person (individual or entity) that provides the software to create and manage wallets, which users can download. A hosted wallet provider is a business that creates and stores a digital currency wallet on behalf of a customer. Most hosted wallets also offer exchange and payments services to facilitate participation in a digital currency system by users.

One of the hallmarks of a virtual currency is that it is anonymous. As a consequence, virtual currencies can be very useful for sanctions evaders. Other features of virtual currencies, including their global nature, distributed structure, limited transparency, and the speed with which transactions can be performed, make them especially suitable for evading sanctions. Significantly, most virtual currency transactions do not pass, at least initially, through the banking system, and so may not be subject to the normal screening. Virtual currencies that are convertible into regular currency present a special problem, as they represent a way to move funds into the regular banking system. Such transactions frequently pass through a money service business (MSB), which can then bundle them with other transactions and convert the funds using the regular banking system. Unfortunately, the use of virtual currencies is still fairly new, so that banks and other entities are still trying to understand how they can be used to evade sanctions. Treasury's Financial Crimes Enforcement Network (FinCen) in the United States has released a comprehensive description of the use of virtual currencies to evade sanctions and launder money; this document is called FIN-2019-A003 Advisory on Illicit Activity Involving Convertible Virtual Currency of May 2019.

Red flags: A transaction performed at least in part in a virtual currency may be used to evade sanctions if

- The transaction is of a regular commercial type that would normally be performed using the normal banking system
- A darknet is involved
- An unregistered peer-to-peer exchange is involved
- The transaction passes through an unregistered foreign MSB
- The transaction is initiated from a non-trusted IP address, or an IP address in a country subject to comprehensive sanctions, such as Iran or Syria

- The transaction is conducted in a virtual currency issued by a country subject to sanctions, such as the Venezuelan petro

Bulk Cash

Commercial transactions and high value transactions are usually conducted through financial institutions using wire transfers and other payment methods. Such transactions are recorded, and can be traced. Cash, on the other hand, is largely untraceable. In most jurisdictions, cash transactions over a certain limit must be reported, but are not necessarily illegal. Moreover, various techniques can be used to accumulate and deposit cash in manner that does not trigger the reporting requirements. The use of bulk cash is therefore a feasible way to move relatively large amounts of money without detection.

Red flags: Red flags for bulk cash as a tool for evading sanctions include

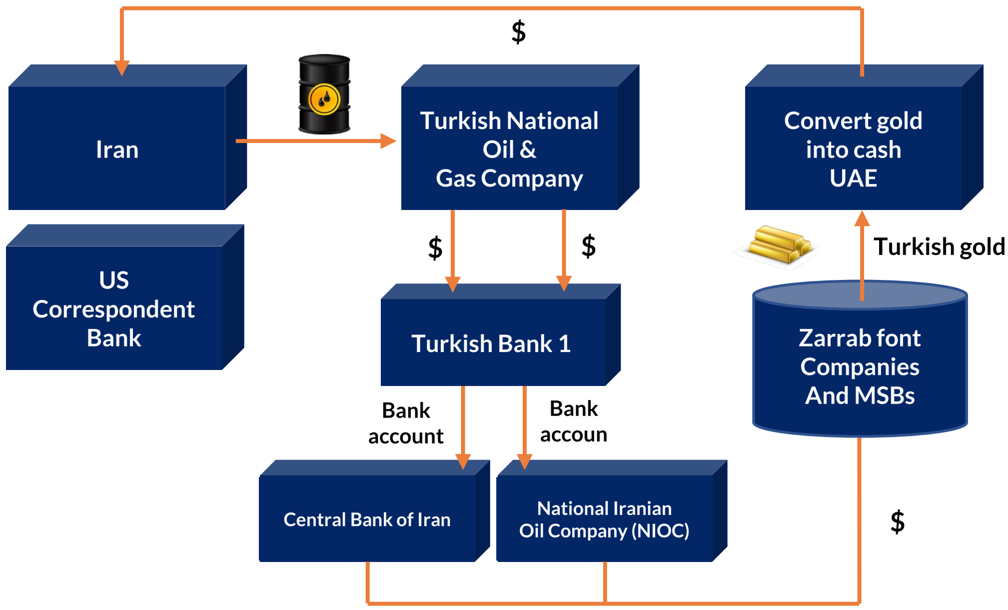
- The use of cash in a transaction that would typically be performed using electronic funds transfers
- Any use of large amounts of cash

Precious Metals

Precious metals represent another widely-accepted store of value that can be used outside the normal banking sector. In many countries, it is acceptable to use gold or, to a lesser extent, silver to move funds.

2017 Case of Reza Zarrab

- Turkish- Iranian gold trader.
- With nine other defendants, including Halkbank CEO Atilla, Zarrab was charged with money laundering, serious bank fraud, and conspiracy to evade U.S. sanctions law against Iran.
- Conspired to disguise oil revenue transactions through the use of false documentation and the export of Turkish gold. Iranian oil companies would deposit oil revenues into a Turkish bank account, which were then used to buy gold in Turkey. That Turkish gold was sent to the UAE, converted to cash, and then sent back to Iran through a U.S. correspondent bank.



Compiled by: https://sanctionsassociation.org/
Source: https://justice.gov/usao-sdny/press-release/file/994976/download

Red flags: Precious metals may be used to evade sanctions if

- The transaction is one that would typically be conducted through wire transfers
- The source of the metals is not evident
- The transaction is conducted in a place geographically close to a sanctioned country, such as in Turkey

Sanction Evasion in the Trade Sector

Sanctioned individuals and entities, and especially sanctioned countries, may have difficulty procuring the goods they need. To circumvent sanctions, they employ a number of different methods. Some of these, such as the use of shell companies and layering purchases through multiple entities, are similar to the techniques used in the financial sector. Others, though, are unique to trade.

Not only maritime shipping companies should take note of the below sanctions evasion techniques and red flags, also related parties such as freight forwarders and commercial insurance companies.

Falsified or Vague Trade Finance Documents

A good deal of international trade is conducted using either letters of credit or collection on documents. Such transactions pass through the normal banking system. One way for evaders to use the system is simply to falsify documents. One common technique is to mislabel the certificate of origin of goods, claiming that they come from a country not subject to sanctions. This may go so far as actually attaching labels to goods, showing a false country of origin. They may show, for example, inaccurate buyers or shipment on different vessels or to different ports from those actually used.

Red flags: Trade finance documentation may have been falsified, or may otherwise be used to obscure the role of a sanctioned party, if

- The terms within the documents are inconsistent (one document says CIF, or example, while another specifies FOB)
- The description of the merchandise is very vague (“electronics”)
- The origin of the goods is from a country other than what would normally be expected
- The destination is vague (“Russia” rather than Sevastopol)
- The transaction includes transshipment with no obvious purpose
- The transaction is inconsistent with one of the parties’ normal business

Voyage Irregularities

Indirect routing, detours or trans-shipment through third countries to obscure origin and destination of vessels.

Complex Ownership or Management Networks

The use of shell companies, matrix business models and organizational structures to disguise ultimate owners or involvement in illicit activity.

Shipments to Ports Close to Sanctioned Countries

Shipment of goods, especially goods subject to extensive sanctions, to ports near a sanctioned country may be a strong indication that sanctions evasion is occurring. The goods will actually be shipped to the port in question, but then transshipped to the sanctioned destination. A prominent example is Dandong, China, which has been identified as a major transshipment point for goods being sent to North Korea in violation of UN and other sanctions. In such cases, the consignee in the first port may simply be an agent or front company, with the end purchaser not appearing in the trade documents.

Red flags: The destination shown may conceal the ultimate destination if

- The port or airport is very close to a country subject to extensive sanctions
- The port is not one to which the buyer would be likely to have the goods shipped

Unusual Merchandise

In general, companies have fairly well-defined lines of business. Even trading companies tend to specialize in certain products. The purchase of goods by a trading company or other buyer that are outside its normal line of business may indicate that the buyer is being used by a sanctions evader to procure goods on its behalf.

Red flags: A trading company or other purchaser inquires about or purchases goods or services outside of its normal line of business.

AIS Record

Sanctions evaders may take various actions to disguise the fact that ships called on certain ports or took on or discharged cargo. All ships carry an Automatic Information System (AIS) transponder that automatically and continually reports their position. While gaps in a vessel's AIS record may be the result of meteorological or other factors, they may also indicate that the transponder was deliberately turned off. This in turn could conceal the ship's location, such as if it called on a port in North Korea.

However, note that a gap in a vessel's AIS transmission could also be caused by weak signals, interference or patchy satellite reception.

Red flags: Unexplained gaps in a vessel's AIS record

Physically Altering a Vessel's Identification

Maritime vessels are required to display their name and International Maritime Organization (IMO) number in a visible location. The IMO number is a unique seven-digit number. A vessel's IMO number is intended to be permanent regardless of a change in a vessel's ownership or name. This allows for identification of the vessel itself. Sanctions evaders may obscure the IMO number, or even change it illegally, to disguise the connection of the vessel to a country subject to sanctions, such as North Korea.

Red flags: Red flags indicating a ship's identification may have been altered include

- Visible evidence that the name and/or IMO number have been painted over or altered
- The IMO or vessel name do not match the IMO records' description of the vessel

False Flag

Falsifying a vessel's flag to mask sanctioned trade. A vessel owner/manager can continue to use a country's flag after it has been struck from the registry, or creating fraudulent national flag registries (ships claiming country flag without authorization).

Ship-to-Ship Transfers

Transferring cargo between vessels while at sea, particularly at night, rather than while located in port to conceal involvement of a sanctioned vessel, or the origin or destination of the cargo.

Ships normally transfer cargoes at ports, where all the equipment necessary is available. However, such transfers will be recorded in the port records. Sanctions evaders may use transfers between two ships at sea to avoid scrutiny.

Definition: Ship to Ship Transfer - Transferring of cargo from one ship to another while at sea rather than while in port.

Red flags: A vessel has cargo that is not included in a manifest or bill of lading

Use of Small/Unregistered Vessels

The use of smaller vessels in ship-to-ship transfers to assist in avoiding recognition by surveillance aircraft.

Case Study: North Korea

As discussed above, North Korea is subject to comprehensive sanctions by the United States. The United Nations has also imposed a variety of sanctions against North Korea. UN sanctions prohibit member states from **importing** a variety of products from North Korea, including:

- Coal
- Textiles
- Seafood
- Iron and iron ore
- Lead and lead ore
- Copper
- Nickel
- Zinc
- Gold
- Silver
- Titanium ore
- Rare earth metals
- Vanadium ore
- Statues and monuments
- Conventional arms
- Food and agricultural products

- Food and agricultural products
- Machinery
- Electrical equipment
- Earth and stone, including magnesia and magnesite
- Wood
- Vessels
- Fishing rights

UN sanctions also prohibit UN members from **exporting** a variety of important goods to North Korea, including:

- Refined petroleum (beyond 500,000 barrels/year)
- Crude oil (beyond 4,000,000 barrels/year)
- Aviation fuel (except fuel required for an aircraft to return to North Korea)
- Rocket fuel
- Condensates and natural gas liquids
- Industrial machinery
- All transportation vehicles (including motor vehicles, trucks, trains, ships, aircraft, helicopters)
- Iron, steel, and other metals
- Conventional arms
- Ballistic missiles
- Weapons of mass destruction and components
- Luxury goods

These sanctions, combined with the financial sanctions imposed on North Korea, largely isolate North Korea from the global economy. Not surprisingly, North Korea has proven very inventive in finding ways to circumvent sanctions. As a UN report in 2016 stated,

> A decade since the adoption of the first resolution, designated entities and associated individuals continue to evade sanctions through increasingly sophisticated and diversified techniques, which include embedding themselves in the transnational networks of foreign partners to conceal their prohibited activities. These entities use multiple locations to gain access to the global trading and banking system, taking advantage of the lack of cooperation between the relevant Member States to evade scrutiny of their activities. Support through diplomatic and embassy staff is a continuing pattern. Importantly, the networks time and again depend on a few trusted key nodes to conduct their business.

The report identifies a number of techniques North Korea uses to evade international sanctions:

- **Sale/export of natural resources:** North Korea sells/exports natural resources (*e.g.*, coal, iron ore, and minerals) to China-based companies, often located near the North Korean border, such as in Liaoning province. The Chinese companies, in turn, sell such natural resources to the Asian market.
- **Indirect payment for natural resources:** Rather than directly paying entities in North Korea, the China- based companies divide their payments into smaller outflows in a complex layering scheme directed to front companies, shell companies, shipping or trade businesses based in Asia (often registered in Hong Kong), and other companies based in various offshore jurisdictions (*e.g.*, British Virgin Islands, Marshall Islands, and the Seychelles). Various financial representatives and corporate service providers may establish the front or shell companies or serve as representatives of the various involved entities.
- **Import and smuggling of goods:** The front or shell companies then use the received payments to purchase and ship commodities to North Korea. These commodity shipments in turn may be used to smuggle goods that the North Korean government uses to build its weapons of mass destruction (WMD) and ballistic missile programs (see below graphic).

A November 2017 FinCEN Advisory on "North Korea's Use of the International Financial System" further explains that these types of trade-based schemes allow the North Korean government to evade U.S. and UN sanctions by directing payments for natural resource sales to its front and shell companies. The North Korean government can then use these laundered proceeds, through its front and shell companies, to access the international financial system and acquire technology for use in its WMD and ballistic missile programs. North Korean representatives often use these companies to establish bank accounts at local banks and take orders from sanctioned North Korean entities.

Treasury believes that the DPRK uses and maintains a network of financial representatives, primarily in China, who operate as agents for North Korean financial institutions. In this capacity, these representatives orchestrate schemes, set up front or shell companies, and manage surreptitious bank accounts to move and disguise illicit funds, evade sanctions, and finance the proliferation of North Korea's WMD and ballistic missile programs.

The U.S. government has recently published a pair of advisories on North Korea and its techniques for evading sanctions, including Department of State/Treasury and Homeland Security July 2018 Advisory "North Korea Sanctions and Enforcement Advisory – Risks for Businesses with Supply Chain Links to North Korea" and Treasury

"North Korea Advisory – Sanctions Risks Related to North Korea's Shipping Practices of February 2018. The agencies describe how U.S. companies can protect themselves from inadvertently buying products produced in North Korea or by North Korean labor. The second details how North Korea evades sanctions on shipping. Both of these advisories are included in the reference materials. The techniques North Korea uses to evade sanctions preventing the import into or the export of goods from North Korea include many of the methods discussed above, including:

- **Sub-contracting:** Foreign suppliers subcontract production to North Korean entities without informing the buyer
- **Mislabeled goods, services, and technology:** North Korean producers affix false country of origin labels showing the product as having been produced somewhere else
- **Joint ventures:** North Korean firms have established hundreds of joint ventures with partners in other countries, especially China, and use the joint ventures to obtain goods, services, and technology in violation of sanctions
- **The sale of raw materials and other goods at artificially low prices:** North Korean exporters sell goods and raw materials well below market prices to intermediaries and other traders, which provides a commercial incentive for the purchase of North Korean goods
- **Information technology services:** North Korea sells a variety of IT services worldwide, using front companies and third-country nationals to conceal the North Korean origin of the services

Similarly, North Korea uses many of the techniques discussed above to allow the shipping of goods to and from North Korea:

- Disabling or manipulating the AIS
- Physically altering vessel identification
- Ship to ship transfers
- Altering vessel and cargo documentation

Summary

- Both targets of sanctions and those who would do business with them have an interest in evading sanctions.
- Banks and other financial institutions regularly screen both customers and transactions to identify and prevent transactions that would violate the applicable sanctions laws
- Methods used to evade sanctions in the financial sector include

- Stripping
- Resubmitting rejected payment messages
- Layering payments
- Using front companies to perform transactions
- Routing transactions through non-bank financial institutions that may have weaker controls
- Paying in virtual currencies, cash, or precious metals
- Methods used to evade sanctions in trade include
- Using front companies
- Altering or forging trade documents
- Arranging for shipment to a legal port close to the sanctioned country
- Disguising or altering the identity of vessels and information regarding their routes
- Ship-to-ship transfers of cargo
- North Korea uses all of these methods, and more, to evade the comprehensive sanctions imposed on it

Review Questions

1. Who would try to evade sanctions?
2. Give five examples of techniques used to evade sanctions in the financial sector.
3. What is stripping?
4. Give three examples of evasion tactics used in the trade sector.
5. Give five examples of tactics North Korea has used to evade sanctions.

ESSENTIAL COMPONENTS OF RISK-BASED SANCTIONS COMPLIANCE PROGRAMS IN DIFFERENT INDUSTRY SETTINGS

Sanctions Compliance Programs: An Introduction

OFAC strongly encourages organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States, U.S. persons, or using U.S.-origin goods or services, to employ a risk-based approach to sanctions compliance by developing, implementing, and routinely updating a sanctions compliance program (SCP).

A Framework for OFAC Compliance Commitments (2019)

Compliance with sanctions laws does not just happen. Full and effective compliance requires the creation, implementation, and operation within an organization of a program to ensure compliance. Indeed, the aim of a sanction compliance program is exactly that – to ensure full and effective compliance with all applicable sanctions laws. In the absence of such a program, an organization could easily find itself in violation, with potentially serious consequences.

There is no "one size fits all" sanctions compliance program. Indeed, neither the European Union nor the United States have imposed specific requirements for a sanctions compliance program. Both have identified the essential components of such a program, though. One thing both emphasize is that the program must reflect the organization's specific risks, so that what constitutes an effective sanctions compliance program will vary greatly. The factors that can affect the program include the organization's location, its size, its business, and whether it engages in substantial cross-border transactions. This chapter will discuss the basic components of an effective sanctions compliance system, and identify specific features of the system which may be necessary for organizations in different industries, including finance, manufacturing, and shipping.

The Essential Components of a Sanctions Compliance System

Neither the EU nor the United States mandate the form and contents of a sanctions compliance program; in fact, neither imposes any legal duty to have such a program. However, both have provided guidance on what the components of an effective sanctions compliance system are likely to include. In addition, the Wolfsberg Group, an association of thirteen global banks which aims to develop frameworks and guidance for the management of financial crime risks, has published recommendations the major features of a sanctions compliance system for financial institutions. The three sets of guidance share many common features, but it is worthwhile to examine them separately, as each covers slightly different issues.

A Framework for OFAC Compliance Commitments

The OFAC guidance, A Framework for OFAC Compliance Commitments, is addressed specifically to compliance with U.S. sanctions. As such, it is a useful source of guidance for any organization doing business with the United States, including selling into the United States, selling U.S. products, purchasing U.S. products, or even simply using U.S. dollars. Beyond this, the OFAC guidance in many ways represents a distillation of international best practices. OFAC has identified five major components:

1. Management commitment
2. Risk assessment
3. Internal controls
4. Testing and auditing
5. Training

Draft EU Guidance on Best Practices for "Internal Compliance Programmes"

The EU guidance is technically directed toward compliance programs for organizations exporting dual use products, and is so primarily concerned with compliance with export controls. However, the guidance addresses sanctions compliance as well, and practically all of the principles and recommendations are applicable to sanctions compliance programs as well. As discussed in Chapter 6 below, sanctions and export control compliance programs have many similarities, and may in fact be part of a single compliance system, so the EU guidance is another relevant source of information. The main components of a compliance program under the EU guidance are:

1. Top-level management commitment to compliance
2. Organization structure, responsibilities and resources commensurate to the entity's risk profile
3. Training and awareness raising
4. Transaction screening process and procedures
5. Performance review, audits, reporting and corrective actions
6. Recordkeeping and documentation

Wolfsberg Guidance on Sanctions Screening

The Wolfsberg Guidance on Sanctions Screening focuses on the role of screening customers and transactions at banks to detect and prevent sanctions violations. The guidance notes, though, that screening is simply one component of a larger sanction program. The components of such a program should include:

1. Policies and procedures
2. Responsible person
3. Risk assessment
4. Internal controls
5. Testing

A link to the Wolfsberg guidance is included in the reference materials.

FFIEC BSA/AML Examination Manual

Other sources contain useful guidance on the necessary components of a sanctions compliance program. For U.S. financial institutions in particular, probably the most important is the **FFIEC BSA/AML Examination Manual**, which is the official manual used by the U.S. government for examining bank's systems for complying with anti-money laundering and sanctions laws.

The manual contains several pages on the OFAC Compliance Program. It starts with a general statement on the OFAC compliance program and then continues with the several pillars of a sound OFAC compliance program. Below are excerpts from the manual:

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 the 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 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, will depend 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 automated clearing house (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".

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 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 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 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 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 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. 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 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 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 will allow 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 will also be useful if 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.

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.

The entire manual is available online at https://bsaaml.ffiec.gov/manual. A link to the individual chapter on compliance with U.S. sanctions laws is included in the reference materials.

The following article from SanctionsAlert, ACSS' newsletter, explains how a review by bank examiners may results in an OFAC enforcement action.

Reviews by bank examiners may result in action by OFAC
Date: August 17, 2016

US financial institutions regularly undergo examinations by federal and state banking agencies, such as the FDIC, OCC, Federal Reserve, as well as their state financial regulator. These "examiners" are tasked with reviewing records, policies, accounts, and documents to evaluate whether an institution's internal procedures are in line with applicable laws and regulations, including those of OFAC. The lack of written safeguards and policies against backlisted persons and entities can be a risky move for banks and other financial institutions.

BSA/AML examinations by bank regulators

Though OFAC regulations do not fall under the scope of AML laws, evaluation of OFAC compliance is frequently included in AML examinations.

The Bank Secrecy Act (BSA) is a federal law that requires banks and other financial institutions to bring large cash transactions and other dubious activity to the attention of regulators. The BSA also requires financial institutions to have complex controls in place to detect any criminal activity, including an "anti-money laundering program". In order to assess compliance with the BSA, and AML laws, an assessment is conducted called the BSA/ AML Examination.

Federal bank regulators conduct formal assessments for adherence to AML laws and the BSA. In order to make sure that the examiners use uniform standards, the Federal Financial Institutions Examination Council (FFIEC), an interagency body, has issued the FFIEC BSA/AML Examination Manual (the Manual). The Manual, first issued in 2005, and last updated in 2014, provides vital information on what to expect from the examiner with respect to their review of an institution's OFAC/sanctions compliance program. Even though OFAC is not part of the FFIEC, it assists in the development of the sections of the manual that relate to OFAC reviews.

OFAC assessment takes a front seat

Despite their name, BSA/AML examinations test for more than just AML compliance. The examination of the compliance program for adherence to OFAC rules by the examiner takes a primary role during the review. In fact, the Manual mentions the word "OFAC" 316 times, including in the first sentence, which reads: "This Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual provides guidance to examiners for carrying out BSA/ AML and Office of Foreign Assets Control examinations." The Manual's section "Core Examination Overview and Procedures for Regulatory Requirements and Related Topics" consists of 14 sections, one of which is entirely devoted to OFAC compliance called "OFAC Overview and Examination Procedures". This section takes up 10% of the Core Procedures, and consists of 11 pages. Based on the number of pages, it is the 2nd largest section, only surpassed by the section on Suspicious Activity Reports.

At the start of the examination, as part of the scoping and planning procedures, the examiner must take a look at the institution's OFAC risk assessment procedures and independent testing.

To facilitate the examiner's understanding of the bank's risk profile and to adequately establish the scope of the OFAC examination, the examiner completes several steps, including:

- **A review of the bank's OFAC risk assessment**. The risk assessment, which may be incorporated into the bank's overall BSA/AML risk assessment, should consider the various types of products, services, customers, entities, transactions, and geographic locations in which the bank is engaged, including those that are processed by, through, or to the bank, to identify potential OFAC exposure. Though not specifically stated in the manual, best practice dictates that a larger financial institution creates a stand-alone OFAC Risk Assessment Policy with an in-depth review of sanctions risks.
- **A review of the bank's independent testing of its OFAC compliance program**. This refers to supporting documents of the independent testing (audit) of the institution's OFAC compliance program. The federal banking agencies' reference to "audit" does not confer an expectation that the required independent testing be done by a specifically designated external or internal auditor, however, the person performing the independent testing must not be involved in any part of the bank's OFAC compliance program. This includes both persons developing policies and procedures and conducting training.
- **A review of the civil penalties area on the OFAC website**. This is to determine whether the bank has had any warning letters, fines, or penalties imposed by OFAC since the most recent examination.
- **A review of correspondence between the bank and OFAC**. The examiner will be looking for relevant communications, including periodic reporting of prohibited transactions to OFAC and, if applicable, annual OFAC reports on blocked property.

OFAC training requirements

The federal bank examiner will ask financial institutions to show evidence of OFAC of training as part of the BSA/AML Examination. According to the Manual, the examiner will:

- request an "OFAC training schedule with dates, attendees, and topics",
- request "a list of persons in positions for which the bank typically requires OFAC training but who did not participate in the training."; and
- "review the adequacy of the bank's OFAC training program based on the bank's OFAC risk assessment."

Potential actions by bank regulators

The federal banking agencies can issue enforcement actions for non-compliance, including requirements to reform the bank's OFAC program and impose civil money penalties.

In a case involving Deutsche Bank AG, the Federal Reserve imposed a $58 million penalty and consent cease and desist order against the German banking giant, related to violations of US sanctions. The 2015 order required Deutsche Bank to implement and enhanced program to ensure global compliance with US sanctions administered by OFAC.

Informing OFAC of irregularities

Federal banking agencies also often have a duty to inform OFAC when they spot problematic behavior, for example involving transactions to or from sanctioned countries or a lack of written controls to comply with sanctions laws.

This duty is usually derived from an agreement made with OFAC called a "Memorandum of Understanding" (MOU). These MOU agreements set forth procedures for the exchange of certain information between the parties, including a full report of the findings during an examination as they relate to sanctions enforcement. Such agreements exist with institutions like the Federal Reserve and the FDIC as well as almost every state financial regulator. For a list of state and federal agencies with which OFAC currently has an MOU, please click here.

The MOU between OFAC and the Federal Reserve, the Federal Deposit Insurance Corporation (FDIC), the National Credit Union (NCUA), the Office of Comptroller of the Currency (OCC) and the now defunct Office of Thrift Supervision (OTS) was signed ten years ago, in 2006. To see it, please click here. Information that can be shared includes unreported violations of sanctions, and other examination findings, such as "significant deficiencies in a banking organization's policies, procedures, and processes for ensuring compliance with OFAC regulations."

OFAC compliance program as a mitigating factor

In identifying a potential sanctions violation, OFAC uses "Enforcement Guidelines," the framework for the enforcement of all economic programs it administers. This document says that OFAC will consider some general factors in determining an enforcement action for an apparent breach of sanctions. One of the factors is General Factor E, Compliance Program: the existence, nature and adequacy of a risk-based OFAC compliance program at the time of the apparent violation, where relevant. OFAC will follow the procedures set forth in the MOU and consults the regulator on the quality and effectiveness of the compliance program in place. Even in the absence of an MOU, OFAC may take into consideration the views of federal, state, or foreign regulators, where relevant. In case of a breach of sanctions laws, having a sound OFAC compliance program can mitigate an OFAC enforcement action.

Salvatore Scotto explains that "OFAC, with its MOUs with various federal, state and other regulators relies on their examinations for insight to a financial institution's ability to effectively comply with the regulations. We are at a state where sanctions programs are more complicated and technology has become more sophisticated, an institution can no longer just buy an off the shelf interdiction tool and issue a compliance policy statement. Sanctions compliance programs require comprehensive governance to meet regulatory expectations. While a regulatory examination can be a bit stressful, the regulators may see something you do not see, embrace their findings as an opportunity to strengthen your sanctions program and hopefully the strength of your sanctions program may one day mitigate an OFAC Enforcement Action".

Another important source are the Superintendent's Banking Regulations of the New York Division of Financial Services (NYDFS) concerning transaction screening. A link is included in the reference materials. Because branches of many major banks, both domestic and international, are located in New York, NYDFS has played a major role in defining the obligations of banks with respect to compliance systems. Although both the AML/BSA Examination Manual and the NYDFS Regulations are focused on banks, many of these points are relevant to compliance systems in other industries as well.

The U.S. Department of Justice investigates and prosecutes especially significant possible violations of U.S. sanctions laws. One thing the Department will consider in deciding whether to apply penalties is the strength of the compliance program of the company being investigated. The Department's Evaluation of Corporate Compliance Programs provides guidance regarding what the Department has concluded a robust sanctions compliance program requires. A link to this document is included in the reference materials.

A comprehensive sanctions compliance program will combine the components from all of these sources, as well as guidance provided by industry groups. Penalty notices and settlement agreements by government authorities identify specific violations, providing still more examples of the sort of issues a robust sanctions compliance system must address.

Management Commitment

Both the EU and the OFAC guidance emphasize the importance of a commitment by senior management to compliance with economic sanctions. The term "senior management" may differ among various organizations, but typically the term should include senior leadership, executives, and/or the board of directors. The OFAC Framework sets out the responsibilities of senior management:

Senior Management's commitment to, and support of, an organization's risk-based SCP is one of the most important factors in determining its success. This support is essential in ensuring the SCP receives adequate resources and is fully integrated into the organization's daily operations, and also helps legitimize the program, empower its personnel, and foster a culture of compliance throughout the organization.

OFAC has identified several steps that are necessary to demonstrate this commitment.

1. Senior management has reviewed and approved the organization's sanctions compliance program.
2. Senior management ensures that compliance units receive sufficient authority and autonomy to act in a manner that effectively controls the organization's OFAC risk.
3. Senior management ensures the existence of direct reporting lines between the SCP function and senior management, including routine and periodic meetings.
4. Senior management takes steps to ensure that the sanctions compliance function receives adequate resources, including human capital, expertise, and information technology. OFAC identifies three criteria for satisfying this requirement.
5. The organization has a designated OFAC compliance officer. This officer can fulfill other functions as well, but overseeing OFAC compliance must be one of their duties.
6. Personnel in sanctions compliance have the necessary knowledge and expertise.
7. Sufficient control functions exist that support the organization's sanctions compliance program, including but not limited to information technology software and systems.
8. Senior management promotes a "culture of compliance" throughout the organization. To establish this culture, the sanctions compliance program should include the following features

9. There is a mechanism for the organization's personnel to report sanctions related misconduct to senior management so that they can do so without fear of reprisal.

10. Senior management takes actions that discourage misconduct and prohibited activities, and highlight the potential repercussions of non-compliance with OFAC sanctions.

11. The sanctions compliance function has the authority to oversee the actions of the entire organization, including senior management, for purposes of sanctions compliance.

12. Senior management demonstrates that it recognizes the seriousness of apparent violations of the sanctions laws, acts against violations, and implements the measures necessary to prevent future violations The EU guidance identifies some additional specific steps, including:

1. Develop a corporate commitment statement stating that the company complies with all EU and Member State dual-use trade control laws and regulations.
2. Define the management's specific compliance expectations and convey the importance and value placed on effective compliance procedures.
3. Clearly and regularly communicate the corporate commitment statement to all employees (also employees with no role in dual-use trade control) in order to promote a culture of compliance with the EU and Member State dual-use export control laws and regulations.

New York DFS Stresses "Tone at the Top"

On June 30, 2016, the New York Department of Financial Services (DFS) issues a final rule on BSA/AML transaction monitoring and OFAC filtering and screening. The regulation includes an annual mandated submission by the Board of Directors or a Senior Officer certifying compliance with the regulations and the measures taken to achieve it.

The rule, effective as of January 1, 2017, applies to all banks, trust companies, savings banks, and savings and loan associations chartered pursuant to the NY Banking Law...and all branches and agencies of foreign banking corporations licensed...to conduct banking operations in New York. The first compliance findings was due April 15, 2018.

An additional step that both demonstrates and enhances management's commitment to sanction compliance is the provision of sanctions training for top management.

Even if all employees receive basic sanctions training, training aimed specifically at top management can explain how sanctions can affect the company and what their responsibilities are.

Directed training is an excellent way to show the commitment of management to sanctions compliance.

Another useful measure is the inclusion of sanctions data in key performance indicators (KPIs). Top management should routinely receive information showing the effectiveness of the company's sanctions compliance system, including transactions and customers rejected and, of course, any violations. A discussion of these KPIs, and of sanctions compliance in general, should be a regular item on board agendas.

Sanctions Risk Assessment

Both the EU and OFAC guidance emphasize the importance of risk assessment in designing and operating a sanctions compliance system. As the EU guidance explains, a sanctions compliance program "needs to be tailored to the size, the structure and scope of the business, and especially, to the company's specific business activity." A risk assessment allows a company to determine its sanctions risk profile, and enables the company to see how each of its units fits into the sanction compliance program. According to OFAC, the risk assessment should address key risk areas, including

1. Customers, supply chain, intermediaries, and counter-parties
2. The products and services the organization offers, including how and where such items fit into other financial or commercial products, services, networks, or systems; and
3. The geographic locations of the organization, as well as its customers, supply chain, intermediaries, and counter-parties.

What Should the RA Exercise Entail?

Source: ACSS OFAC Essentials Online Certificate Course

The ultimate aim of the assessment is to identify vulnerabilities and risks so that the company can implement ways to mitigate them into the sanctions compliance program. The risk assessment should be designed to detect the particular types of misconduct most likely to occur in a particular corporation's line of business" and regulatory environment. OFAC has provided a good deal of detail on what the risk assessment should cover and how it should be conducted:

1. The organization conducts, or will conduct, an OFAC risk assessment in a manner, and with a frequency, that adequately accounts for the potential risks. Such risks could be posed by its clients and customers, products, services, supply chain, intermediaries, counter-parties, transactions, and geographic locations, depending on the nature of the organization. As appropriate, the risk assessment will be updated to account for the root causes of any apparent violations or systemic deficiencies identified by the organization during the routine course of business.
2. In assessing its OFAC risk, organizations should leverage existing information to inform the process. In turn, the risk assessment will generally inform the extent of the due diligence efforts at various points in a relationship or in a transaction. This may include:
   a. On-boarding: The organization develops a sanctions risk rating for customers, customer groups, or account relationships, as appropriate, by leveraging information provided by the customer (for example, through a Know Your Customer or Customer Due Diligence process) and independent research conducted by the organization at the initiation of the customer relationship. This information will guide the timing and scope of future due diligence efforts.
   b. Mergers and Acquisitions (M&A): As noted above, proper risk assessments should include and encompass a variety of factors and data points for each organization. One of the multitude of

areas organizations should include in their risk assessments—which, in recent years, appears to have presented numerous challenges with respect to OFAC sanctions—are mergers and acquisitions. Compliance functions should also be integrated into the merger, acquisition, and integration process. Whether in an advisory capacity or as a participant, the organization engages in appropriate due diligence to ensure that sanctions-related issues are identified, escalated to the relevant senior levels, addressed prior to the conclusion of any transaction, and incorporated into the organization's risk assessment process. After an M&A transaction is completed, the organization's Audit and Testing function will be critical to identifying any additional sanctions-related issues.

3. The organization has developed a methodology to identify, analyze, and address the particular risks it identifies. As appropriate, the risk assessment will be updated to account for the conduct and root causes of any apparent violations or systemic deficiencies identified by the organization during the routine course of business, for example, through a testing or audit function.

While the nature and scope of the risk assessment will vary, any risk assessment should take the following factors into account:

- Locations of the institution's businesses
- The institution's size
- Staffing (both compliance and otherwise)
- Governance: how the institution is managed
- The institution's businesses, including the services and products it offers
- The details of the institution's operations
- Its customers
- Counterparties
- Other business relations and their locations

The purposes of a risk assessment are to identify the sanctions risks an organization faces and to enable it to determine how best to mitigate those risks. It is unlikely that an organization will be able to eliminate risk completely. Rather, it may decide to classify risks. It can apply its risk assessment methodology to a customer, for example, and then decide whether the customer is low, medium, or high risk. The procedures and requirements applying to the customer may vary according to the risk classification. Onboarding a low-risk customer may not need any approval at all, for example, while accepting a medium-risk customer requires a review by Compliance, and a high-risk customer a decision by higher management.

Risk assessment is not a one-time thing. An organization certainly needs an initial risk assessment when it first sets about designing a sanctions compliance system. The organization should regularly update the risk assessment, either on a periodic basis or in response to developments in the organizations business or in sanctions laws.

Organizational Structure and Internal Controls

Effectively complying with sanctions laws requires an organization to create and allocate the human, technical, and organizational resources needed. The sanctions compliance The EU guidance states that an organization should have a structure that "allows for conducting internal compliance controls."

Organizational Structure

Every organization needs some sort of structure for complying with its sanctions obligations. The structure can vary greatly across organizations, depending upon their size, business, location, and level of sophistication. Compliance does not necessarily require individuals or units within the organization specifically dedicated solely to sanctions compliance. It does require, though, that the organization

1. Identify its sanctions risks,
2. Determine how best to mitigate those risks, and
3. Design and implement a structure that assigns personnel and resources to sanctions compliance.

The EU guidance gives a number of steps that will help ensure that the organization's internal structure can be effective in ensuring sanctions compliance. These steps are:

1. Determine the number of sanctions compliance staff (legal and technical).
2. Entrust at least one person in the company with the company's sanctions compliance, and ensure that an equally qualified substitute can assume the task in case of absence (sickness, holidays etcetera). Depending on the average volume of orders, this person may only have to handle tasks relating to sanctions compliance on a part-time basis.
3. Clearly identify, define and assign all compliance related functions, duties and responsibilities. An organizational chart may be useful in doing this. Clearly identify back-up functions whenever possible.
4. Make sure that the internal organizational structure for sanctions compliance is known throughout the organization. Make the contact details of the responsible person sanctions questions known within the company. If sanctions compliance duties are being outsourced, the interface to and the communication with the company needs to be organized.
5. Define the knowledge and skills needed by legal and technical dual-use trade control staff. Job descriptions are recommended.

6. Make sure that sanctions compliance staff is protected from conflicts of interest.
7. Locate the responsibility for compliance in a suitable department or division. This may involve personnel in one department – Legal – for example, authorizing transactions by another department. Enable this staff to function as expert advisors to guide company decisions resulting in compliant transactions.
8. Draw up a compliance manual to describe the operational and organizational processes that must be followed by the dual-use export control staff and other affected employees.

The structure an organization creates to ensure compliance with sanctions depends upon the unique characteristics of the organization. Some organizations, such as large international banks, have a department specifically dedicated to sanctions compliance, with other personnel responsible for compliance spread throughout the organization. In smaller organizations, sanctions compliance may be one of a number of duties a team member has. In any case, the organization should designate one person as being specifically responsible for the overall operation of the sanctions compliance system, even if many others are involved, and even if that team member has other duties as well.

While there is no “one size fits all” solution for sanctions compliance, larger organizations usually adopt a “three lines of defense” model, where responsibility for sanctions compliance is distributed throughout the organization. The three lines of defense are:

1. **First Line:** The business, which is responsible initially for reviewing customers and transactions for possible sanctions issues, and for making the initial decision about whether to proceed with a customer or transaction.
2. **Second Line:** Compliance, fills a number of vital functions, including
3. Reviewing decisions by the business
4. Answering questions and responding to requests for guidance
5. Periodically reviewing compliance decisions by the business
6. Creating, maintaining and updating the organizations sanctions policies and procedures
7. **Third Line:** Audit (either internal or external), which regularly reviews the operation of the entire sanctions compliance system.

Policies and Procedures

As well as a compliance structure, an organization needs policies and procedures detailing how it mitigates sanctions risks and addresses specific situations. The OFAC guidance provides the following guidelines for these policies and procedures:

1. The organization has designed and implemented written policies and procedures outlining the SCP. These policies and procedures are relevant to the organization, capture the organization's day-to-day operations and procedures, are easy to follow, and designed to prevent employees from engaging in misconduct.
2. The organization has implemented internal controls that adequately address the results of its OFAC risk assessment and profile. These internal controls should enable the organization to clearly and effectively identify, interdict, escalate, and report to appropriate personnel within the organization transactions and activity that may be prohibited by OFAC. To the extent information technology solutions factor into the organization's internal controls, the organization has selected and calibrated the solutions in a manner that is appropriate to address the organization's risk profile and compliance needs, and the organization routinely tests the solutions to ensure effectiveness.
3. The organization enforces the policies and procedures it implements as part of its OFAC compliance internal controls through internal and/or external audits.
4. The organization ensures that its OFAC-related recordkeeping policies and procedures adequately account for its requirements pursuant to the sanctions programs administered by OFAC.
5. The organization ensures that, upon learning of a weakness in its internal controls pertaining to OFAC compliance, it will take immediate and effective action, to the extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated.
6. The organization has clearly communicated the SCP's policies and procedures to all relevant staff, including personnel within the SCP program, as well as relevant gatekeepers and business units operating in high-risk areas (e.g., customer acquisition, payments, sales, etc.) and to external parties performing SCP responsibilities on behalf of the organization.
7. The organization has appointed personnel for integrating the SCP's policies and procedures into the daily operations of the company or corporation. This process includes consultations with relevant business units, and confirms the organization's employees understand the policies and procedures.

While the OFAC guidance refers to internal controls, policies, and procedures, it provides relatively little direction regarding what those policies and procedures should be. In general, policies are broad statements regarding how the organization addresses various compliance issues. Procedures refer to specific methods for dealing with various situations.

Compliance Policy

The first component of internal controls is a general sanctions policy. A policy is a statement of corporate intent or series of commitments of the company.. Such policies in connection with sanctions compliance are usually adopted by the Board of Directors or Senior Management of the organization, who are then deemed responsible and accountable for that policy. The purpose of creating an sanctions policy is to communicate to the organization and the general public the organization's stance towards sanctions compliance. The contents of a sanctions compliance policy can vary, but generally include:

- A purpose statement, outlining why the organization is issuing the policy, and what its desired effect or outcome of the policy should be.
- An applicability and scope statement, describing who the policy affects and which actions are impacted by the policy. The applicability and scope may expressly exclude certain people, organizations, or actions from the policy requirements. Applicability and scope is used to focus the policy on only the desired targets, and avoid unintended consequences where possible.
- An effective date which indicates when the policy comes into force.
- A responsibilities section, indicating which parties and organizations are responsible for carrying out individual policy statements. Many policies may require the establishment of some ongoing function or action. For example, a third party supplier policy might specify that a purchasing office be created to process purchase requests, and that this office would be responsible for ongoing actions. Responsibilities often include identification of any relevant oversight and/or governance structures.

The compliance policy may address general matters, such as whether the organization will do business with certain countries or involving certain types of products, such as arms or nuclear materials. The sanctions compliance policy may include provisions regarding

- The organization's commitment to compliance with the letter and spirit of applicable laws
- The organization's decision to comply with other measures, such as the sanctions laws of other countries and industry best practices
- The organization's willingness to provide sufficient resources for compliance with sanctions laws and regulations
- Cooperation with the agencies that administer the sanctions or export controls program, law enforcement and investigating authorities where necessary
- Respect for client confidentiality, which should be breached only where necessary
- Clearly defined responsibilities and accountabilities for sanctions compliance within the business

- The parameters within the company is willing to operate which defines what business the company will and, more importantly, will not, accept
- The acceptance of new business subject to compliance with appropriate Customer Due Diligence (CDD) and risk assessment procedures
- The continuation of existing business only where such business complies with appropriate CDD, sanctions regimes, risk assessment and monitoring procedures
- The approach to the education, training and awareness maintenance of all staff and management
- Recognition of the importance that staff promptly report their suspicions of any sanctions violation internally
- The organization’s attitude towards persistent non-compliance with sanctions procedures, and
- A positive indication of the cultural and moral attitude that the organization wishes to create towards compliance with sanctions regimes and contributions towards national security.

To implement the compliance policy, the organization should:

- Circulate a summary of the financial institution or company’s approach to assessing and managing its OFAC/sanctions risk
- Allocate of responsibilities to specific persons department and functions
- Circulate a summary of the firm’s procedures for carrying out appropriate identification and monitoring checks in line with their risk-based approach, and
- Circulate a summary of the appropriate monitoring arrangements in place to ensure that the firm’s OFAC/sanctions policies and procedures are being carried out.
- Circulate a summary of license, blocking, reporting and rejecting duties.

Procedures

Procedures are documents detailing how issues are handled and responsibilities performed. Neither the EU nor the OFAC guidance require specific procedures. An effective sanctions compliance program will require at least the following procedures. This list is by no means exhaustive; rather, it represents the basic procedures a compliance program should include:

1. **The allocation of compliance responsibilities.** This procedure identifies who or where in the organization is responsible for various aspects of sanctions compliance.
2. **Monitoring of changes to the applicable laws and other relevant developments.** Sanctions laws change frequently. In addition, external developments, such as political changes in a country, can also have sanctions implications. There must be a way for the organization to monitor changes in sanctions laws and relevant developments on an

ongoing basis; to revise policies and procedures as necessary; and to communicate those changes to the rest of the organization.

3. Risk assessment methodology, timing, etc.
4. **Review of existing policies and procedures in light of the results of risk assessments.** It is important that policies and procedures reflect the findings of risk assessments. This requires a procedure for reviewing existing policies and procedures after a risk assessment has been completed. Ideally, this will happen at least once a year.
5. **Customer due diligence.** To mitigate sanctions risks, it may be necessary to conduct some sort of due diligence regarding customers and potential customers, to ensure that they are not subject to sanctions. This issue is covered in detail in Chapter 6 below on screening.
6. **Review and approval of individual transactions.** Depending upon the nature of an organization's business, it may be advisable to review at least some types of transactions that present a potential sanctions risk, and to require some sort of non-routine approval of medium- and high-risk transactions.
7. **Assignment of risk classification.** Classifying customers, business relations, and transactions as low, medium, or high risk allows an organization to devote its sanctions compliance resources to focusing on the riskiest. This requires a procedure explaining when and how the organization applies a risk classification.
8. **Applying for a license.** If the organization ever decided to do business with sanctioned countries, entities, or individuals, it may need a license to do so. This in turn requires a procedure that defines who makes the decision to apply for a license, and who is responsible for the application.
9. **Maintaining information on what sanctions licenses and exemptions apply to the organization's business.** Conversely, if licenses or exemptions apply to an organization's business, there must be readily available information within the organization regarding the scope of the license or exemption, as well as what procedures are required with respect to customers or transactions involving the license or exemption.
10. **Handling transactions where a license authorizes an otherwise-prohibited activity.** Transactions subject to a license may require special measures, such as reporting to the authorities. This procedure should specify those measures.
11. **Rejecting customers or transactions, including what the customer or counterparty should be told.** Inherent in the review of customers and transactions is the possibility that customers will be declined or transactions rejected. A procedure should identify who makes these decisions and what the customer or other parties are told about the decision. In general, it is considered wise to say as little as possible, so as not to give potential sanctions evaders any information about how an organization makes decisions regarding sanctions compliance.

12. **Resolving disputes within the organization.** Different parts of an organization may disagree over matters of sanctions compliance, such as whether a customer or transaction should be rejected. A procedure can specify how such disputes are resolved.
13. **Blocking (freezing) transactions and administering frozen property.** Persons in the EU, the United States, and other countries may be required by national law to freeze the funds or other assets of sanctioned parties. A procedure should identify when an asset must be frozen; exactly what the process is for freezing it (by placing in a special account, for example); and how the property is handled while it is frozen.
14. **Records retention.** U.S. law, for example, requires that records regarding transactions potentially subject to sanctions be kept for five years. In addition, many organizations have their own records retention policies. The records retention procedure should identify
    a. What records must be retained
    b. How they will be retained (electronically, hard copy)
    c. How long they must be retained
    d. What should be done with them after the retention period has ended
15. **Training.** The procedure should specify who is responsible for preparing and providing training; what types of training will be provided; who is to receive training and on what schedule; and what records of training should be maintained.
16. **Periodic review (audit).** The performance of periodic reviews of the operation of the sanctions compliance system requires its own detailed set of procedures. While Audit may be primarily responsible, the involvement of the compliance and legal functions is also necessary to ensure that the audit procedures reflect the legal requirements applying to the organization.
17. **"Whistleblower" procedures.** There must be a procedure that enables personnel to report possible sanctions violations or practices against organization policy anonymously and without fear of retribution
18. **Internal investigations.** The first step when a potential violation of sanctions laws or the organization's policies and procedures is uncovered is to conduct an internal investigation. The procedure should specify when such an investigation should occur; who has the power to initiate it; who conducts the investigation; what the procedures for the investigation are; the form of the final report; who the report goes to; and who has the power to act upon the report.
19. **Reporting (both regular and of potential or actual violations).** As discussed above, regular reporting to management about the operation of the sanctions compliance system is highly advisable. This may include such Key Performance Indicators as the number of transactions reviewed, the number rejected, the number of apparent violations observed, etc. In addition, a separate procedure should describe reports of potential violations.

20. **Reporting to regulators.** Depending upon national law, organizations may be required to report to regulators instances where they have frozen assets or rejected transactions. A procedure should provide the details for this.
21. **Voluntary disclosures.** There may be times when an organization decides to voluntarily disclose to the appropriate authorities potential sanctions violations. The voluntary disclosure procedure should provide the details for this, including who has the authority to make a disclosure and what the disclosure should contain.
22. Correcting weaknesses in the sanctions compliance system. Audits and internal investigations may identify deficiencies in the sanctions compliance system. A procedure should ensure that, after the completion of an audit or an internal investigation, any deficiencies identified in the sanctions compliance system are corrected.
23. Communications with clients. Communication with clients on sanctions matters is a delicate issue. An organization may want customers to understand its overall policies, such as a refusal to do business with specific countries. However, it should not divulge too much information regarding either the overall operation of its sanctions compliance system or how it handles individual transactions, as such information can help sanctions evaders. The communications procedure should detail what information will be provided to clients and business partners, especially with respect to individual transactions.
24. Coordination of sanctions policies within a corporate group. Members of a corporate group may well be located in different countries and subject to different sanctions regimes. It is important that a policy or procedure describe how they shall coordinate policies, and in particular whether and to what extent subsidiaries must comply with the sanctions laws of the corporate parent. OFAC has repeatedly penalized U.S. companies for violations of U.S. sanctions by their foreign affiliates.

Testing and Audit

Periodic testing of the performance of the sanctions compliance system is essential. As the EU guidance explains,

> Performance reviews and audits verify whether the ICP is implemented to operational satisfaction and is consistent with the applicable national and EU export control requirements. A well-functioning ICP has clear reporting procedures about the notification and escalation actions of employees when a suspected or known incident of non-compliance has occurred. As part of a sound compliance culture, employees must feel confident and reassured when they raise questions or report concerns about compliance in good faith. Performance reviews,

audits and reporting procedures are designed to detect inconsistencies to clarify and revise routines if they (risk to) result in non-compliance.

Testing and audit can either be performed internally or by an outside body. Similarly, the testing may be specific to the sanctions compliance function, or conducted as part of an enterprise-wide review. According to OFAC, an in-depth audit of each department in the bank should probably be conducted at least once a year. What is essential is that the testing cover sanctions compliance, and that it fulfill certain basic criteria, as identified by OFAC:

1. The organization commits to ensuring that the testing or audit function is accountable to senior management, is independent of the audited activities and functions, and has sufficient authority, skills, expertise, resources, and authority within the organization.
2. The organization commits to ensuring that it employs testing or audit procedures appropriate to the level and sophistication of its SCP and that this function, whether deployed internally or by an external party, reflects a comprehensive and objective assessment of the organization's OFAC-related risk assessment and internal controls.
3. The organization ensures that, upon learning of a confirmed negative testing result or audit finding pertaining to its SCP, it will take immediate and effective action, to the extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated.

No matter who conducts the audit, the individuals performing audits should have a well-developed understanding of the applicable sanctions laws, the company's risk profile, and the company's relevant policies and procedures.

The contents of testing will naturally vary by the organization and the structure of its compliance system. Among other forms of testing, auditors can analyze customer and transaction records and sales data to confirm that the company has not engaged in prohibited transactions or accepting customers outside of its risk profile. If a company utilizes a screening software, the auditor should verify that the restricted party screening is operating effectively and that the company has developed an effective way to establish whether potential hits are actual matches or false positives.

Training

Training is the final essential component of an effective sanctions compliance system.

The EU guidance includes the following recommendations with respect to training:

1. Provide compulsory, periodic training for all sanctions compliance staff to ensure they possess the knowledge to be compliant with the regulations and the company's ICP.
2. Ensure via training that all concerned employees are aware of all relevant dual-use trade control laws, regulations, policies, control lists and all amendments to them as soon as they are made public by the competent authorities. If possible, consider customized trainings.
3. Develop general awareness raising for all employees and dedicated training activities for e.g. purchasing, engineering, project management, shipping, customer care and invoicing.
4. Consider, whenever appropriate, to make use of national or EU training initiatives.
5. Incorporate lessons learnt from performance reviews, audits, reporting and corrective actions, whenever possible, in your training or export awareness programs.

The OFAC guidance elaborates on these points in terms of commitments by the organization to training. While OFAC speaks in terms of an OFAC-related compliance program, these principles apply to all sanctions compliance programs, regardless of the applicable sanctions:

1. The organization commits to ensuring that its OFAC-related training program provides adequate information and instruction to employees and, as appropriate, stakeholders (for example, clients, suppliers, business partners, and counterparties) in order to support the organization's OFAC compliance efforts. Such training should be further tailored to high-risk employees within the organization.
2. The organization commits to provide OFAC-related training with a scope that is appropriate for the products and services it offers; the customers, clients, and partner relationships it maintains; and the geographic regions in which it operates.
3. The organization commits to providing OFAC-related training with a frequency that is appropriate based on its OFAC risk assessment and risk profile.
4. The organization commits to ensuring that, upon learning of a confirmed negative testing result or audit finding, or other deficiency pertaining to its SCP, it will take immediate and effective action to provide training to or other corrective action with respect to relevant personnel.
5. The organization's training program includes easily accessible resources and materials that are available to all applicable personnel.

This guidance leaves organizations a great deal of flexibility in deciding who and how to train. Training may be on-line or in person. At a minimum, though, an organization should consider these categories of training:

1. **General sanctions training for all employees.** This training familiarizes employees with the general requirements of sanctions law, as well as the organization's policies and procedures.
2. **Specialized training for employees with responsibilities that may require them to make sanctions decisions.** These may include sales and marketing personnel, order processing, exports, and legal. If testing of the system is being performed internally, audit should receive specialized training as well. The nature and content of the training called for will vary by function.
3. **Detailed training for compliance staff.** No matter how the sanctions function is staffed, its personnel require a high degree of knowledge. They should receive detailed training on the applicable laws and on the requirements for the various aspects of the organization's operations.
4. **Sanctions training for top management**. Violating sanctions can have very negative consequences for an organization. Training directed at upper management, including corporate boards, will sensitize them to the importance of sanctions compliance and demonstrate the importance of compliance to the rest of the organization.

It is important to keep complete records of sanctions training, so that the organization can demonstrate to audit and to any government regulators that adequate and relevant training is being provided. At the least, training documentation should show

1. The names and titles of persons receiving training
2. What type of training was received (general, specialized, senior management, etc.)
3. The date of the training
4. How the training was provided (live or on-line).

Customer Due Diligence

Customer due diligence is also an important pillar of a sound sanctions compliance program, especially in the light of the OFAC 50% Rule.

OFAC 50% Guidance

- Because OFAC's lists are not exhaustive
- Issued February 2008, revised August 2014
- https://www.treasury.gov/resource-center/sanctions/Documents/licensing_guidance.pdf
- An Entity that is owned 50% or greater by a sanctions target is treated as a sanctions target.
- Underscores the need for thorough due diligence

The OFAC guidance, revised in 2014, states that the property and interests in property of **entities directly or indirectly owned 50 percent or more in the aggregate by one or more blocked persons are considered blocked regardless of whether such entities appear on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) or the annex to an Executive order.** The revised guidance expands upon the earlier guidance by addressing entities owned 50 percent or more in the aggregate by more than one blocked person.

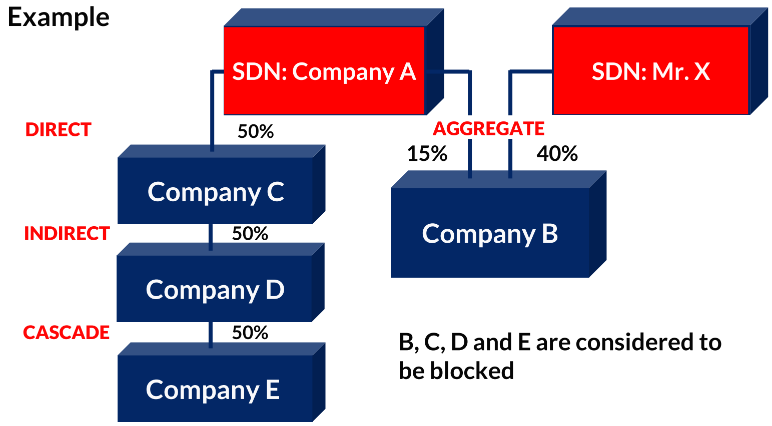
Note that

- OFAC's 50% rule speaks only to ownership and not control. An entity that is controlled (but not owned 50 percent or more) by one or more blocked persons is not considered automatically blocked pursuant to OFAC's 50 Percent Rule. (note however: A U.S. persons should be careful when conducting business with non-blocked entities in which blocked individuals are involved; U.S. persons may not, for example, enter into contracts that are signed by a blocked individual. See OFAC FAQ 398).
- OFAC also applies a 50 percent rule to entities on the Sectoral Sanctions Identifications List (SSI List) created in July 2014 in the Ukraine-/Russia-related sanctions context. The property and interests in property of persons on the SSI List (and entities owned 50 percent or more in the aggregate by one or more persons subject to the SSI List restrictions) are not required to be blocked; instead a more limited set of transaction restrictions applies to them. In the context of the SSI List restrictions, therefore, these FAQs can be used to identify which subordinate entities are subject to the SSI List restrictions only and are not meant to suggest that any additional actions (such as blocking) apply to those entities.

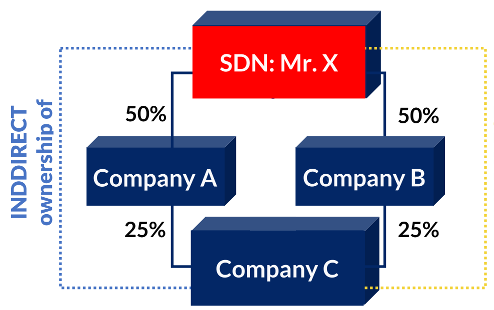
OFAC has issued Frequently Asked Questions (FAQs) to respond to inquiries relating to the status of entities owned by individuals or entities whose property and interests in property are blocked under Executive orders and regulations administered by OFAC (blocked persons). These FAQs provide additional clarity regarding revised guidance that OFAC issued on August 13, 2014, amending earlier guidance that had been issued on February 14, 2008 (OFAC's 50 Percent Rule).

Examples:

OFAC 50% Guidance and Indirect Ownership in Complex Ownership



Source: ACCS OFAC Essentials Online Certificate Course



A and **B** are considered to be blocked

C is considered to be blocked. This is so because of two reasons:

1. INDIRECT: through its 50% ownership in A, Mr. X is considered to indirectly own 25% in C; and through its 50% ownership in b, Mr. X is considered to indirectly own 25% in C. When Mr. X's indirect ownership of C through A and B is totaled, it equals 50%.

2. DIRECT: C is also considered to be blocked due to the 50% aggregate ownership by A and B, which are themselves blocked entities due to Mr. X's 50% ownership of each.

Source: ACCS OFAC Essentials Online Certificate Course

Considerations for Specific Industries

The creation of a compliance program of course depends upon the organization's risk assessment. While risks vary even between companies within the same industry, certain risks are prevalent throughout certain industries. OFAC has provided guidance for the financial and securities industries in particular in the form of a risk matrix. The risk matrix identifies certain types of common risks, and shows the circumstances under which the risk should be considered low, medium, or high.

Finance

Because of its central role in the global economy, the financial sector also plays a pivotal role in sanctions compliance. The following are some of the activities carried out by banks and other financial institutions that may pose an additional risk of potential sanctions violations:

- 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

OFAC has released the following matrix showing the risks associated with particular types of customers and transactions that financial institutions can use to evaluate their sanctions compliance systems. While this risk matrix was developed specifically for financial institutions, the same principles and conclusions may apply to other industries as well

Low Risk	**Moderate Risk**	**High Risk**
Stable, well-known customer base in a localized environment	Customer base changing due to branching, merger, or acquisition in the domestic market	A large, fluctuating client base in an international environment.
Few high-risk customers; these may include nonresident aliens, foreign customers (including accounts with U.S. powers of attorney), and foreign commercial customers	A moderate number of high-risk customers	A large number of high-risk customers.
No overseas branches and no correspondent accounts with foreign banks	Overseas branches or correspondent accounts with foreign banks	Overseas branches or multiple correspondent accounts with foreign banks.

Low Risk	Moderate Risk	High Risk
No electronic services (*e.g.*, e-banking) offered, or products available are purely informational or non-transactional	The institution offers limited electronic (*e.g.*, e-banking) products and services	The institution offers a wide array of electronic (*e.g.*, e-banking) products and services (*i.e.*, account transfers, e-bill payment, or accounts opened via the Internet).
Limited number of funds transfers for customers and non-customers, limited third-party transactions, and no international funds transfers	A moderate number of funds transfers, mostly for customers. Possibly, a few international funds transfers from personal or business accounts	A high number of customer and non-customer funds transfers, including international funds transfers.
No other types of international transactions, such as trade finance, cross-border ACH, and management of sovereign debt	Limited other types of international transactions	A high number of other types of international transactions.
No history of OFAC actions. No evidence of apparent violation or circumstances that might lead to a violation	A small number of recent actions (*i.e.*, actions within the last five years) by OFAC, including notice letters, or civil money penalties, with evidence that the institution addressed the issues and is not at risk of similar violations in the future	Multiple recent actions by OFAC, where the institution has not addressed the issues, thus leading to an increased risk of the institution undertaking similar violations in the future.
Management has fully assessed the institution's level of risk based on its customer base and	Management exhibits a reasonable understanding of the key aspects of OFAC	Management does not understand, or has chosen to ignore, key aspects of OFAC

Low Risk	Moderate Risk	High Risk
product lines. This understanding of risk and strong commitment to OFAC compliance is satisfactorily communicated throughout the organization	compliance and its commitment is generally clear and satisfactorily communicated throughout the organization, but it may lack a program appropriately tailored to risk	compliance risk. The importance of compliance is not emphasized or communicated throughout the organization.
The board of directors, or board committee, has approved an OFAC compliance program that includes policies, procedures, controls, and information systems that are adequate, and consistent with the institution's OFAC risk profile	The board has approved an OFAC compliance program that includes most of the appropriate policies, procedures, controls, and information systems necessary to ensure compliance, but some weaknesses are noted	The board has not approved an OFAC compliance program, or policies, procedures, controls, and information systems are significantly deficient.
Staffing levels appear adequate to properly execute the OFAC compliance program	Staffing levels appear generally adequate, but some deficiencies are noted	Management has failed to provide appropriate staffing levels to handle workload.
Authority and accountability for OFAC compliance are clearly defined and enforced, including the designation of a qualified OFAC officer	Authority and accountability are defined, but some refinements are needed. A qualified OFAC officer has been designated	Authority and accountability for compliance have not been clearly established. No OFAC compliance officer, or an unqualified one, has been appointed. The role of the OFAC officer is unclear.
Training is appropriate and effective based on the institution's risk	Training is conducted and management provides adequate resources	Training is sporadic and does not cover important regulatory

Low Risk	Moderate Risk	High Risk
profile, covers applicable personnel, and provides necessary up-to-date information and resources to ensure compliance	given the risk profile of the organization; however, some areas are not covered within the training program	and risk areas or is nonexistent.
The institution employs strong quality control methods	The institution employs limited quality control methods	The institution does not employ quality control methods.

Financial institutions should of course have all of the procedures identified above. In addition, they should implement the following procedures as well, which can address at least some of the risks identified above:

Certain additional procedures are advisable for the finance industry in particular:

1. Screening transactions. Banks may handle transactions through a variety of different systems, depending upon whether the transaction is purely domestic, regional (as with SEPA in Europe), or international (through the SWIFT system). The bank's procedures should specify which types of payments and other messages are screened. The procedures should also identify what types of transactions are screened, and how.
2. A policy prohibiting stripping. OFAC has repeatedly imposed very large penalties on foreign banks for stripping. Every financial institution needs a policy strictly prohibiting stripping, with procedures describing how to determine if stripping has occurred.
3. Detection of resubmitted payments. As discussed above, one way individuals or entities may seek to evade sanctions is to resubmit a transaction, such as a payment, with altered names. The financial institution should have a procedure in place for identifying payments that appear to have been resubmitted with changed information, stopping those payments, and taking action against the parties involved.
4. A policy regarding cover payments, and in particular, which SWIFT message types are used for cover payments. Because parties have used cover payments to disguise the involvement of sanctioned parties in a transaction, most international banks now use the MT202 COV message as the primary if not only means of transmitting cover payments between banks.
5. A policy regarding transactions through sundry or own accounts. Unfortunately, personnel within banks have sometimes cooperated

with sanctions evaders to use nostro, sundry, and other "own" accounts within the bank to process transactions. Because such transactions are considered to take place within the bank itself, they may not be subject to the regular screening. A policy should set out whether such transactions are screened, and what measures are necessary to ensure that these accounts are not used to evade sanctions.

6. A policy regarding book-to-book transactions. Book-to-book transactions are between two customers of the same bank, so that the transaction occurs only on the bank's books, without any external flow of funds. This procedure should state whether such transactions must be screened or, if not, what the basis of the decision not to screen was.
7. Screening procedures for securities transactions. While securities transactions may occur through the SWIFT network, they do not always pass through a bank's normal transaction screening system. There should be procedures in place to ensure that securities transactions are subject to screening.
8. Screening and other procedures re securities custody. Securities custody presents its own sanctions challenges, as ownership may not be immediately evident and as securities transactions may not go through the institution's normal screening system. This means specific procedures for securities custody are advisable.
9. The integration of sanctions policies and procedures into trade finance. Trade finance is a major business for many banks, large and small. Trade finance exposes financial institutions to additional risks beyond normal payments and credit transactions. Any party to a trade transaction, including the shipper, vessel, and insurer, could be subject to sanctions. In addition, the merchandise itself can raise sanctions issues. It is essential that sanctions policies be fulling integrated into trade finance, and that the trade finance function have detailed procedures for addressing sanctions issues.
10. Responding to questions from correspondent banks. Correspondent banks frequently inquire about individual transactions, as well as about a bank's overall compliance policies, procedures, and structures. There should be a specific procedure setting out who is responsible for responding to these inquiries, and in general how they are handled.

Securities

OFAC has identified certain common types of sanctions risks in the securities industry, and recommended measures to protect against those risks. OFAC recommends that U.S. financial institution weigh several factors with regard to its due diligence review of a customer or intermediary:

- The nature of the customer – its location, market, products and downstream customers;
- The type, purpose, and activity of the account;
- The nature and duration of the relationship of a foreign institution with the U.S. financial institution;
- Applicable sanctions regulations and supervisory/enforcement regime (including anti-money laundering laws) governing a foreign institution; and
- Information that can be obtained regarding the institution's sanctions compliance record.

OFAC has identified a number of risk factors for securities transactions:

1. International transactions, including wire transfers
    a. A high number of international transactions, cross-border transactions, or investments in a foreign investment fund or on a foreign exchange;
    b. The presence of overseas branches or multiple correspondent accounts with foreign financial institutions, including correspondent accounts subject to enhanced due diligence under Section 312 of the USA PATRIOT Act.
2. Foreign customers/accounts:
    a. A large, fluctuating client base across a number of foreign jurisdictions involving a large number of security transactions;
    b. Customers located in or having accounts in high-risk jurisdictions, such as countries found to be of "primary money laundering concern" pursuant to Section 311 of the USA PATRIOT Act;
    c. Customers located in or having accounts in countries that are havens for money laundering or are inadequately regulated, including countries identified by the Financial Action Task Force as maintaining an inadequate AML/CFT regime;
    d. Customers located in or having accounts in countries where local laws, regulations, or provisions (such as privacy laws) prevent or limit the collection of client identification information;
    e. Customers located in an offshore financial center as identified by the U.S. Department of State;
    f. Accounts for senior political or government officials of a foreign government;
    g. Accounts of closely held corporations;
    h. Accounts for unregistered or unregulated investment vehicles;
    i. Accounts for non-resident aliens;
    j. Accounts maintained at an offshore bank.
3. Foreign broker-dealers who are not subject to OFAC regulations:
    a. Lack of information regarding beneficial owners of securities; and
    b. Foreign broker-dealers that act as introducing brokers.
4. Risks of investments in foreign securities: practical exposure increases when investing in a foreign investment fund or foreign exchange,

because of the risk that the securities are issued by a sanctioned country or party or otherwise in violation of OFAC sanctions, e.g., securities of an issuer that provides financing for a sanctions target. Other risk factors include:
   a. Cross-border settlements involving the interaction of different settlement systems and laws in different countries;
   b. Foreign securities that may be more prone to misidentification in the course of a trade, e.g., similar names between two foreign issuers;
   c. Foreign companies that issue shares in bearer form.

5. Personal investment corporations or personal holding companies
   a. Beneficial ownership by a non-U.S. person that maintains a private banking account with a U.S. financial institution.

6. Very high net worth institutional accounts, hedge funds, funds of hedge funds and other alternative investment funds (private equity, venture capital funds) and intermediary relationships:
   a. Lack of transparency regarding securities/investments and beneficial owners;
   b. U.S. hedge fund with an offshore related fund where beneficial owners are offshore investors; and
   c. Subscription funds that originate from or are routed through an account maintained at an offshore bank, or a bank organized or chartered in an inadequately supervised and poorly regulated jurisdiction, or a foreign shell bank.

7. Omnibus accounts/use of intermediaries:
   a. Potential for the use of code names to invest funds in the United States on behalf of sanctions targets, concealing the identities of the beneficial owners;
   b. Accounts for intermediaries held in street name that trade on behalf of third parties, such as other broker-dealers, banks, and mutual funds; and
   c. Cross-border trades executed for unregulated investment vehicles, e.g., hedge funds, private equity funds, and other private pools of capital.

8. Third-Party introduced business:
   a. Business introduced by an overseas bank, affiliate, or other investor based in high risk or inadequately regulated countries.

9. Confidential accounts:
   a. Private banking accounts established or maintained for non-U.S. persons or services, including financial and related services, to wealthy clients who use offshore accounts for tax avoidance purposes.

The Maritime Shipping Industry

The shipping industry faces especially complicated sanctions risks. In this context, the "shipping industry" includes, not just companies operating ships, but all the related services, including chartering, insurance, freight forwarding, loading and unloading, bunkering, and repair services. In August 2019, ACSS published an article describing the complexities of sanctions compliance in the shipping industry. Find the article here: https://sanctionsassociation.org/the-complexities-of-sanctions-compliance-risk-in-the-shipping-industry/.

Along with the normal risks factors, such as the identity of the parties to transactions and the origin and destination of goods, the nature of the commodities being shipped can pose a particular sanctions risk. Examples of commodities that may pose particular sanctions (and export control) risks include:

- Military items
- Dual-use items, including nuclear, biochemical, WMD, missile technology
- Drug precursors and certain general chemicals
- Otherwise bulk standard generic items that become an issue because of a targeted sanction on a single country.

OFAC and the United Nations released several documents that provide guidance on behavior that might indicate red flags for maritime sanctions evasion and offer clues as to what information should be gathered to “know your shipping customer.” The organizations advise institutions to look for and mitigate risks associated with business lines, high-risk areas, and shipping practices such as record-keeping and ship-to-ship transfers.

While certainly not exhaustive, the overview below adapted from their guidance is intended as a first line of sight for people in the US-centered financial services industry.

Low	Moderate	High
Customer can produce all transport documents (i.e. bills of lading, air waybills) including: • shipping companies • consignees • notify parties • forwarding agents • ports of loading • ports of discharge • ports of transshipment • final destinations • shipping vessels • air carriers	Customer can produce most transport documents.	Customer can produce little to no transport documents.

Low	Moderate	High
The customer has robust document record-keeping practices that include • Customer account information • End-user statements, or similar language • Export licenses, if applicable • Shipping/freight forwarder documentation	The customer has robust record-keeping methods that include customer account information.	Customer does not have record-keeping practices.
Customer does not conduct business in “high-risk” areas such as Syria or North Korea.	Customer may conduct business in high-risk areas but has strong record-keeping practices.	Conducts business in “high-risk areas” and near “suspicious ports.”
Company does not conduct business in high-risk business lines.	Company conducts business in high-risk business lines but has all documentation and strong record-keeping practices.	Company conducts business in high-risk business lines and has lax documentation and record-keeping practices.
Vessels perform “ship to ship” transfer, do not do any high-risk business and has no gaps in Automated Information System (AIS) transmission data.	Vessels perform “ship to ship” transfers but do not do business in high-risk areas or business lines. Or, if they do, have clear business reasons to do so and has no gaps in AIS history.	Vessels perform “ship to ship” transfers, company does business in high-risk areas or industries and has poor record-keeping practices.
Newer vessel with recent high scores on port control safety	Older vessels with recent high scores on port control safety	Older vessels with poor history of poor scores on port control

Low	Moderate	High
inspections and no fines for pollutions.	inspections and no fines for pollutions.	safety inspections and/or fines for pollution.
No instances of vessel name changes or changes in registration (reflagging).	A couple of instances of "reflagging" with clear business reasons.	Frequent "reflagging" and/or changes in vessel name.
Clear and well documented IMO number history and AIS transmission data with no instances of "going dark" or lapses in location monitoring.	A few instances of "going dark" but not near suspicious ports or high-risk areas and with clear explanations as to why.	History of "going dark" in high-risk areas.

OFAC has also identified a number of measures the shipping industry can take to mitigate these risks. It did so most recently in an advisory regarding attempts by Iran to ship petroleum in defiance of U.S. sanctions. A copy of this advisory is included in the reference materials. While this advice was directed specifically towards petroleum shipping and Iran, the principles apply throughout the shipping industry:

1. **Insurance:** There is sanctions risk related to the provision of underwriting services or insurance or reinsurance to certain Iranian energy- or maritime-related persons or activity. In particular, persons who knowingly provide underwriting services or insurance or reinsurance to any Iranian person on the SDN List — such as NIOC, NITC, or IRISL — are exposed to sanctions. Additionally, transactions involving the designated entity Kish Protection & Indemnity Club (aka Kish P&I),

a major Iranian insurance provider, are considered sanctionable activity. The United States is not alone in its concerns with Kish P&I. Many countries' flagging registries do not accept vessels insured by Kish P&I to their registries.

2. **Verify cargo origin:** Individuals and entities receiving petroleum or petroleum products shipments should conduct appropriate due diligence to corroborate the origin of such goods when transported or delivered by vessels exhibiting deceptive behaviors or where connections to sanctioned persons or locations are suspected. Testing samples of the cargo's composition can reveal chemical signatures unique to Iranian oil fields. Publicizing cases where certificates of origin are known to be falsified can deter efforts to resell the goods to alternative customers.
3. **Strengthen Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) compliance:** Financial institutions and companies are strongly encouraged to employ risk mitigation measures consistent with Financial Action Task Force standards designed to combat money laundering, and terrorist and proliferation financing. This includes the adoption of appropriate due diligence policies and procedures by financial institutions and non-financial gatekeepers and promoting beneficial ownership transparency for legal entities, particularly as related to the scenarios outlined above.
4. **Monitor for AIS manipulation:** Ship registries, insurers, charterers, vessel owners, or port operators should consider investigating vessels that appear to have turned off their AIS while operating in the Mediterranean and Red Seas and near China. Any other signs of manipulating AIS transponders should be considered red flags for potential illicit activity and should be investigated fully prior to continuing to provide services to, processing transactions involving, or engaging in other activities with such vessels.
5. **Review all applicable shipping documentation:** Individuals and entities processing transactions pertaining to shipments potentially involving petroleum or petroleum products from Iran should ensure that they request and review complete and accurate shipping documentation. Such shipping documentation should reflect the details of the underlying voyage and reflect the relevant vessel(s), flagging, cargo, origin, and

destination. Any indication that shipping documentation has been manipulated should be considered a red flag for potential illicit activity and should be investigated fully prior to continuing with the transaction. In addition, documents related to STS transfers should demonstrate that the underlying goods were delivered to the port listed on the shipping documentation.

6. **Know Your Customer (KYC):** As a standard practice, those involved in the maritime petroleum shipping community, including vessel owners and operators, are advised to conduct KYC due diligence. KYC due diligence helps to ensure that those in the maritime petroleum shipping community are aware of the activities and transactions they engage in, as well as the parties, geographies, and country-of-origin and destination of the goods involved in any underlying shipments. This includes not only researching companies and individuals, but also the vessels, vessel owners, and operators involved in any contracts, shipments, or related maritime commerce. Best practices for conducting KYC on a vessel include researching its IMO number, which may provide a more comprehensive picture of the vessel's history, travel patterns, ties to illicit activities, actors, or regimes, and potential sanctions risks associated with the vessel or its owners or operators.
7. **Clear communication with international partners:** Parties to a shipping transaction may be subject to different sanctions regimes depending on the parties and jurisdictions involved, so clear communication is a critical step for international transactions. Discussing applicable sanctions frameworks with parties to a transaction can ensure more effective compliance.
8. **Leverage available resources:** There are several organizations that provide commercial shipping data, such as ship location, ship registry information, and ship flagging information. This data should be incorporated into due diligence best practices, along with available information from OFAC as outlined below in the "Sanctions Resources" section of this advisory.

Commercial (re) insurance

The (re)insurance market provides significant support to the global maritime industry. For this reasons, there is a risk to this sector of exposure to prohibited or sanctionable activity.

Whilst obtaining commercial insurance is not likely to be the primary goal of those involved in the movement of illicit goods, it can be exploited to obtain the necessary permits to initiate voyages and enter ports to transfer prohibited goods.

In addition, sanctions are constantly changing, so insurance companies should review existing policies to ensure that procedures are in place to mitigate the risk of certain regional exposures to sanctions. An example is the 2014 sanctions against Ukraine after Russia's annexation of Crimea.

Marsh and McLennan provides the guidance with respect to assessing potential impact of the Crimea sanctions upon clients' global insurance programs, in particular organizations that do business with Russia and/or Ukraine.

They may wish to consider the following practical questions:

1. Does the organization have a mechanism for identifying whether any of its global operations are doing business with individuals or businesses that may be the subject of government sanctions?

   Consider whether the company screens its clients and payees against trade sanctions watch lists.

2. Do any of the organization's operations have contact with or interact with the individuals or businesses that are the subject(s) or the existing government sanctions or with companies owned or controlled by such persons?

   If the answer is "yes," immediately seek the advice of legal counsel to ensure compliance with sanctions.

3. Are the organization's international operations aware of sanctions and is there a plan in place to ensure operational compliance with existing sanctions and/or potential further sanctions?

   Creating and maintaining clear lines of communication with international subsidiaries can help to ensure alignment of purpose and may speed identification and resolution of any business activities that may not be fully compliant with sanctions.

4. Will the organization be able to make recoveries under an insurance policy if there are sanctions?

   Coverage under any insurance policy is always subject to laws as well as the terms and conditions of the policy. On a broad basis, if a law or regulation prohibits an insurer from making payments under a policy, then that prohibition likely will supersede any policy language and expectation of payment.

5. Do the organization's current insurance policies contain exclusions or cancellation wording involving sanctions?

   Insurance policies may exclude or limit coverage due to sanctions, or call for policy termination in the event of sanctions. These provisions vary from policy to policy. Multinational organizations should review the terms and conditions of their insurance policies to better understand how each will respond.

6. Does the organization currently purchase political risk, trade credit, or other types of insurance that may be called upon in the event of loss due to escalating tensions in the region?

   Multinational organizations should pay special attention to analyzing such policies, which may have reporting obligations that require them to report situations that are likely to give rise to a loss — or could include conditions that require them to cease new shipments. Organizations should maintain an open line of communication with insurance underwriters to obtain any necessary approval before taking actions to minimize loss. For trade credit insurance, it is important to monitor approved buyer credit limits to watch for insurer limit reductions and cancellations.

7. Does the organization rely upon suppliers (or customers) that may be affected by the existing or future sanctions?

   The risk issues associated with sanctions may go well beyond an organization's own operations. Multinational organizations may wish to identify alternative suppliers of critical materials or services in order to ensure continuity of business.

https://www.marsh.com/us/insights/research/sanctions-risk-management-viewpoint.html

Lloyd's, another insurance firm, headquartered in London, also provides guidance on sanctions compliance for the insurance sector.

This section contains information from Lloyd's Market Bulletin Ref Y5246 of April 2019.

Lloyd's bulletin says that the (re)insurance industry is characterized by a division of responsibility between brokers, insurers and reinsurers but each party in the placement chain is individually liable for sanctions compliance.

In line with the Lloyd's guidance, market participants are expected to understand their sanctions risk profile, and review their current sanctions due diligence and screening processes to validate that they are proportionate to their risk profile.

Due diligence and screening procedures should be risk-based and proportional to a (re)insurer's sanctions risk profile. When assessing their exposure to sanctions risk, Lloyd's Market Bulletin suggested that (re)insurers refer to the below table of non-exhaustive risk factors.

Table 1: Considerations when evaluating sanctions risk profile:

Risk category	Risk factor	Example of simple risk	Example of complex risk
Jurisdiction risk	Geographical location of asset/risk	North Sea, Atlantic Ocean	Yellow Sea, East and South China Sea, Sea of Japan, Mediterranean and Red Seas, Gulf of Tonkin, Persian Gulf (See Table 2 below)
	Geographical location (re)insured	EU, US	DPRK, China, Taiwan, Russia, Singapore, Hong Kong
	Legal and regulatory obligations (consider which sanctions laws and regulations are applicable to carrier / broker)	Parties in placement chain are subject to requirements from only one jurisdiction (e.g. all in the UK) and/or are based in non-sanctioned country	Parties in placement chain are subject to requirements from different or multiple jurisdictions (e.g. UK broker, Chinese carrier, US/EU reinsurer), and/or are based or proximal to sanctioned country
Product risk	Class of business (consider likely activities, goods,	Non-marine, property, motor	Marine hull and cargo, marine chartering

Risk category	Risk factor	Example of simple risk	Example of complex risk
	equipment, services or trade covered)		
	Type of product	Food, humanitarian medical supplies	Crude oil, coal, refined petroleum, iron, steel, zinc products, or dual use goods, goods subject to export control
Client/customer risk	Type of policyholder (consider corporate structure, ownership and control, and operational structure of (re)insured)) Counterparty risk	Multinational, high degree of compliance activity and transparency over extends only to named policyholder(s)	Small company with limited trading history Cover could extend to persons/entities not identified at the point of underwriting

Lloyd's says that when validating whether due diligence and screening processes are proportional to a (re)insurer's risk profile, the following considerations may also be noted:

Direct vs. Reinsurance

It is accepted that **direct insurers** (and potentially facultative reinsurers) will be better placed than treaty reinsurers to:

- Seek pre-bind information from the insured/broker – insurers are expected to understand the underlying entities involved in a risk and their activities, and prior to binding a policy should, at a minimum, ensure that they have obtained sufficient information to make a robust determination of a risk's profile.
- Consider whether additional compliance controls may assist in meeting regulatory expectations for higher risk exposures – for example, pre-bind review of a vessel's AIS history could assist in identifying unusual patterns of activity of clients operating in and around high-risk geographical areas. Commercial data / software is now readily available for carriers that have high-regional exposures.

Whilst **reinsurers** (particularly treaty reinsurance underwriters) are further removed than direct insurers from meaningful insight into the activities of the insured parties, regulators will expect them (and direct insurers) to demonstrate the below:

- Clear communication with counterparties – setting out any sanctions compliance conditions with local cedants and brokers, including regional offices and coverholders.
- Relevant available resources utilized – there is a wide range of information available from the UN, OFAC, the US Coast Guard and numerous organizations that provide commercial shipping data (e.g. ship registry information).

Lead or follow (re)insurers

The lead (re)insurer, as the party primarily interacting with the broker, will be better placed to identify potential red flags and engage with the broker to obtain additional information on a risk. However both lead and follow (re)insurers have the same compliance obligations and should be aware of this guidance.

Delegated authorities

Any delegation of sanctions due diligence should be reflected in full detail in the contractual arrangements with the third party coverholder / TPA. (Re)insurers should ensure that the third-party performs activities and services to a high standard and no less a standard than would have been undertaken by the (re)insurer itself.

(Re)insurers are also reminded that where they rely on the outsourced activities or services of third-parties to perform sanctions due diligence and screening on their behalf, they are not legally absolved from liability for breaches.

Sources of information and role of brokers

As outlined in UK Treasury's Office of Financial Sanctions Implementation (OFSI) Guidance (March 2018), it is OFSI's view that brokers should be well placed to obtain sufficient placement information to conduct appropriate sanctions checks against clients and insurance beneficiaries when cover is issued. While it is reasonable for (re)insurers to request brokers to liaise with their clients and request the placing information that the underwriter requires to conduct their sanctions due diligence, the specific requirements that a (re)insurer applies to the broker in respect of sanctions compliance are a matter for the parties to contract.

Where brokers have obtained such placing information to comply with their own sanctions obligations, (re)insurers can ask to see that placing information, but they may also wish to seek further information to ensure that they comply with their own sanctions obligations (which may differ from the broker's sanctions obligations). In accordance with their risk-based procedures, (re)insurers should verify that the placement information remains accurate and complete. Where high-risk factors exist, brokers should, to the best of their ability, ensure that due diligence information is provided to underwriters in sufficient time to enable them to consider it and raise further queries.

Red flags – when is enhanced due diligence triggered?

To assist the market in identifying higher risk exposure, Lloyd's has compiled the below non-exhaustive list of risk factors. Whilst these risk factors are not themselves illegal or prohibited, they have been present in previous cases of sanctionable activity.

Lloyd's suggests that the presence of the primary risk factor, a **geographical high-risk** location, combined with any other risk factor (secondary risk factor), may raise a red flag that triggers enhanced due diligence procedures. If enhanced due diligence measures do not mitigate the level of perceived risk, consideration should be given as to whether it is prudent to proceed with the provision of cover.

Primary risk factor		Secondary risk factor	
Type of risk	**Description**	**Type of risk**	**Description**
Geographical high risk	Risks with exposures in the geographical areas known for illicit marine activity (including but not limited to the East China Sea, Yellow Sea, Sea of Japan, Mediterranean and Red Seas, Gulf of Tonkin, Persian Gulf/ Hormuz Straits) and proximity to sanctioned territories	Type of product	Coal, refined petroleum, iron, steel, zinc products, military goods and dual use goods subject to The Export Control Order 2008 (or Export Control legislation)
		Automatic Identification System (AIS) anomalies	Historical and lengthy disruption of the vessel's AIS, particularly when coupled with exposures in geographical areas deemed as high risk.
		Ownership and/or management complexities	A complex corporate vessel ownership structure (particularly if based/proximal to a high-risk area) and chartering vessels to third parties, when combined with other secondary red flags, may trigger further due diligence.

Primary risk factor		Secondary risk factor	
Type of risk	**Description**	**Type of risk**	**Description**
	(see **Appendix C**)	Flag changes/ 'flags of convenience'	Frequent change of vessel flag, particularly if registered under 'flags of convenience' (where a vessel is registered in a state that is different to that of the vessel owner), where combined with other secondary red flags.
		Document inconsistencies	Inaccuracies or lack of detailed information in product descriptions.

Appendix C

North Korea – high risk geographical locations

The OFAC Advisory, Updated Guidance on Addressing North Korea's Illicit Shipping Practices (21 March 2019), included the below regional map where ship-to-ship transfers of refined petroleum commonly occur – sea names have been added for ease of reference.

Graphic extracted from p.3 of the OFAC Advisory, Updated Guidance on Addressing North Korea's Illicit Shipping Practices, 21 March 2019.

Enhanced due diligence (EDD) procedures

Lloyd's also explains that where EDD and screening has been identified as necessary, (re)insurers / brokers are encouraged to seek a full explanation of contractual arrangements which could give rise to increased sanctions risks.

More specifically, due diligence checks should not merely seek to eliminate obvious links to i) 'North Korea' or 'Syria' or ii) any identified designated parties. It may be appropriate for an in-depth "activity-based" assessment of a client (also at renewal and for any extensions) to be conducted to lead to a clear understanding of the risk profile, often referred to as "network analysis". The importance of this network analysis is apparent in cases of sanctions evasion.

Lloyd's provides the following case example to demonstrate the importance of network analysis.

DPRK Sanctions Evasion Example

Lighthouse Winmore and Billions No.18

In December 2017, the UN Security Council listed four ships, on its North Korea Sanctions List. Hong Kong-flagged Lighthouse Winmore and Panama-flagged Billions No. 18 were found to have transferred marine diesel to DPRK-flagged tankers, Sam Jong 2 and Rye Song Gang I on 19 October 2017. Both tankers engaged in activity to conceal vessel movements including switching off their Automatic Identification System a few days before and after the transfers.

Network Analysis

The Lighthouse Winmore was chartered the month before the ship-to-ship transfers by the Marshall Islands company, Oceanic Enterprise Ltd, via a Singapore-based broker. Its sole director and shareholder is Shih-Hsien Chen, a national of Taiwan Province of China. The Yingjen Fishery Company communicated administrative and logistical arrangements to the owner via the broker, while the Billions Bunker Group Corporation issued operational instructions to the captain.

The UN Panel of Experts noted that the owner/operator of the Lighthouse Winmore, Lighthouse Ship Management (also involved in ship-to-ship transfers), was previously known as the similar-sounding Billion Great International Group Ltd, suggesting a link to Chen's companies. In addition, two of Chen's tankers, the Lighthouse Winmore and the Golden Rich, both use the same document of compliance holder and International Safety Management manager1, Vanguard Shipping Safety Management Consultant Co. Ltd, which is the owner and operator of another tanker engaging in ship-to-ship transfers, the Jin Hye.

At the time of the 5 March 2018 Report from the UN Security Council Panel of Experts established pursuant to resolution 1874 (2009), the Panel were continuing to investigate Shih-Hsien Chen's central role in transfers of petroleum products to the DPRK. The Panel underscored the DPRK's reliance on trusted foreign nationals to continue to conduct illicit activities.

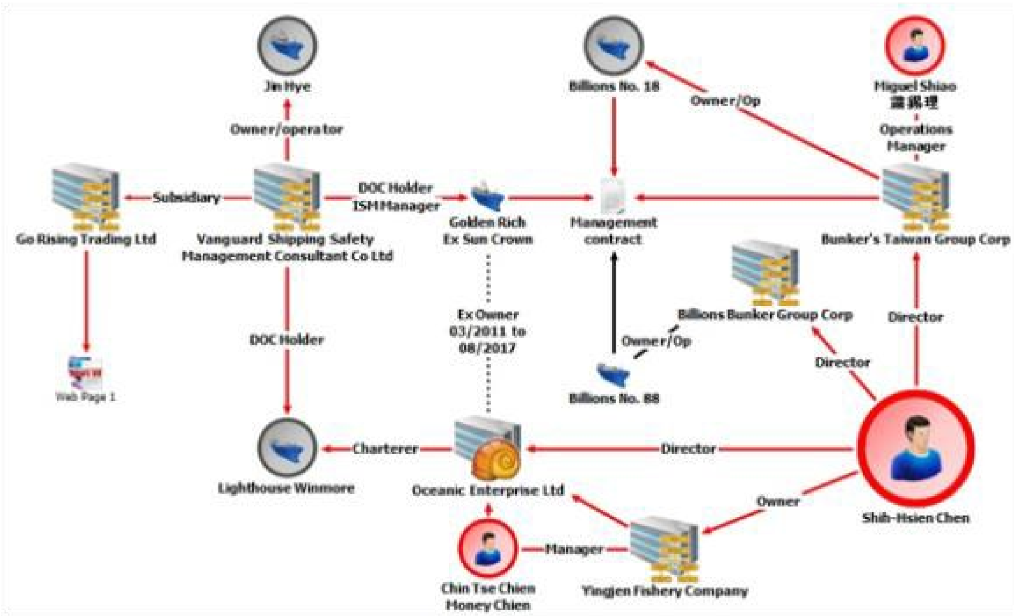


Figure XV extracted from p.33 of the Report of the UN Security Council Panel of Experts established pursuant to resolution 1874 (2009), distributed 5 March 2018.

KOTI

Panama-flagged product tanker Koti was seized at Pyeongtaek-Dangjin port, south of Incheon by the South Korean authorities in December 2017, as the vessel was believed to have transferred oil products to the DPRK despite international sanctions. In a similar pattern used in the above cases of Lighthouse Winmore and Billions No. 18, the Koti departed from Yeosu and selectively used its Automatic Identification System for several days from 30 November 2017 to conceal its location.

Circumstances may arise where a (re)insurer considers it necessary to further verify the information they obtained during the due diligence process. In these instances, they may choose to do so by obtaining independent authoritative documentary evidence which corroborates the information relating to the named (re)insureds, other parties and/or trade to which the (re)insurance may relate. (Re)insurers should consider whether conducting further supply chain analysis could lead to a clearer understanding of the risk profile – for example by asking questions on intended use of goods and seeking to identify end-user(s).

Lloyd's underscores that re(insurers) should adopt a risk-based approach when determining what enhanced due diligence measures should be undertaken and provides the below example of an enhanced due diligence questionnaire.

Example enhanced due diligence questions

Insureds and counterparties	
Name of insureds	(direct insurance only)
Name of all parties covered under contract of (re)insurance	
Name of ultimate beneficial owners/controller(s) of ships	
Have the above names been screened against UN, EU, US, UK sanctions lists?	
Vessel activity	
Has the ship been screened against UN, EU, US, UK sanctions list/higher risk vessels named in relevant OFAC Advisories?	
How is the ship managed	
How is the ship crewed	
Where is the ship flagged	
What are the trading activities of the ship (are there any details on previous trading activities)	(consider whether the vessel has engaged in ship-to-ship transfers, sailed to high risk geographical locations, been known to turn off AIS in such locations etc.)
Supply chain analysis	
Details of the nature of the trade, the identity of the goods, equipment or services – and the identity of parties involved in such trade/supplies.	

Location/origin of goods/equipment.	
Intended use and/ or end-user/specification/modification of goods/equipment.	
Identities of intermediaries involved in the handling of the goods/equipment.	
Payments	
Identity of part/parties who will be making payments (including premium)	(is this is different from the named (re)insured, to ascertain the position under sanctions)

Controls

Use of sanctions clauses

Lloyd's explains that while the inclusion of sanctions limitation and exclusion clauses can provide (re)insurers with a degree of legal protection if illicit activity is detected post-bind, (re)insurers are reminded that an adequate sanctions clause may suspend liability but might not extinguish liability.

As such, the use of such clauses should not be considered as a substitute for the due diligence and pre-bind screening processes detailed in the Lloyd's guidance.

Similarly, a direct insurer may seek, as a prudent measure, to introduce warranties (contractual clauses) that aim to restrict higher risk activity (such as deviations in voyages or the disablement/ manipulation of a vessel's AIS) and warranties which promote continuous AIS broadcast (promoting compliance with the international convention on Safety Of Life At Sea (SOLAS). However this should be considered as part of the insurer's risk-based and holistic due diligence and screening program.

Training

(Re)insurers should ensure that they implement and maintain effective and up-to-date training designed to ensure that all staff, especially relevant underwriters and claims staff in higher-risk classes (as identified above), are aware of this guidance, know what red flags to look for, and understand the controls in place.

Any such training should be formal and administered on a regular basis particularly as sanctions evasion techniques continue to evolve. It is important that training is extended to regional teams where the need to mitigate elevated sanctions exposure risk is greater.

Technology

There are numerous software products available to support carriers / brokers with due diligence, tracking and screening. (Re)insurers should determine whether their sanctions risk profile could warrant the need for commercial tracking/ intelligence providers that could be utilized for EDD, screening and ongoing monitoring. Where vessel screening / tracking tools are already being used for underwriting purposes to rate, or charge a premium, for a risk, it may be useful to encourage its use by the compliance function particularly for EDD checks or monitoring.

Where vessel data is utilized, (re)insurers should note that this data has some limitations, and should therefore be analyzed in conjunction with other information sources to build an accurate picture to inform underwriting / claim judgements.

Ongoing monitoring and reporting

(Re)insurers should ensure that their sanctions compliance processes and controls are documented, kept regularly updated and are regularly reviewed. (Re)insurers are asked to consider subjecting their sanctions compliance processes and procedures to testing, gap analysis and internal audit on a regular basis to ensure that they are operating as they should.

(Re)insurers are also reminded that their internal reporting procedures should be aligned to their reporting obligations as, for example, outlined in UK HM Treasury's Office of Financial Sanctions Implementation (OFSI) Guidance (March 2018). The obligation to report voluntarily to OFSI is in addition to any other non-financial sanctions reporting obligations you may have. These could include submitting Suspicious Activity Reports (SARs) to the National Crime Agency (NCA) under the Proceeds of Crime Act 2002, making disclosures of potential breaches of export control legislation to UK HMRC and notifying the Financial Conduct Authority (FCA) if related to a failure of systems and controls. In some cases, there may be specific obligations to report under section 19 of the Terrorism Act 2000. Note that reporting to your regulator or submitting a SAR does not meet your reporting obligations under financial sanctions. If you have information to report regarding financial sanctions, this must be sent to OFSI: ofsi@hmtreasury.gsi.gov.uk or, for other countries, to your local regulator.

Exporters and importers

Companies involved in international trade, such as exporters and importers are particularly vulnerable for sanctions violations.

The below article from SanctionsAlert, the ACSS newsletter, provides vital sanctions compliance lessons to U.S. exporters when dealing with Iran.

OFAC's $1.5M Epsilon Fine Provides Four Vital Lessons to U.S. Exporters to Iran
October 3, 2018

On September 13, 2018, Epsilon Electronics Inc, a car audio and video equipment manufacturer, agreed to pay the U.S. Treasury's Office of Foreign Assets Control (OFAC) $1,500,000 to settle a case related to alleged violations of the Iranian Transactions and Sanctions Regulations.

The case, which is a culmination of a 2014 penalty notice and two court cases, contains four vital lessons for U.S. exporters whose products may be found in Iran.

The September 2018 settlement is a re-consideration of a disputed penalty notice from 2014, at which time OFAC fined Epsilon $4,000,000. In the 2014 notice, OFAC alleges that from 2008 to 2012, the electronics manufacturer broke the law by selling audio and video equipment to Asra International, LLC. Epsilon sold these goods despite having reason to know that Asra International, a company incorporated in Dubai, UAE, would more than likely distribute the goods to Iran.

In 2016, Epsilon challenged OFAC's 2014 Penalty Notice in court. Epsilon lost their case, but upon appeal, the case was sent back to OFAC for reconsideration. The latest settlement is the result of this "reconsideration".

Lesson 1: Conduct CDD on Foreign Distributor Who May not be Similarly Restricted in Doing Business with Iran

The case underscores the importance of proper due diligence with regard to foreign distributors that are not similarly restricted under their local law in doing business with Iran.

Some of the 39 invoices involving Epsilon's Iran sanctions violations were issued through a distributor of Epsilon, namely; Power Acoustik Electronics, Inc.

According to the 2016 court documents, Power Acoustik allegedly sent a shipment to Iran in 2008. When OFAC found out about the shipment, it promptly issued a subpoena on Power Acoustik. Power Acoustic responded to OFAC that it had no knowledge of the shipment. OFAC closed the investigation with the issuance of a cautionary letter in January 2012. In this letter, OFAC told Power Acoustik that the regulations "prohibit virtually all direct or indirect commercial financial or trade transactions with Iran by U.S. persons (...)", and that the 2008 shipment appears to have violated the regulations. OFAC also told Power Acoustic that it could "take further action in the future should additional information warrant renewed attention."

Despite this warning from OFAC, five more transactions took place from Epsilon to Asra International following OFAC's 2012 cautionary letter.

Though OFAC did not find direct evidence that the Epsilon shipments to Asra International subsequently made their way into Iran, the agency did find some evidence that the Dubai-based company was shipping goods to Iran regularly. On their website, in an English-language "about us" tab, it indicated that Asra International and Asra Electronic Trading held "10 long years of experience in Iran's car audio and video market". The website also listed an address in Iran for Asra Electronic Trading, which OFAC discovered was the same address listed on the airway bill for the 2008 shipment of goods from Power Acoustik to Iran.

The U.S. District Court for the District of Columbia issued an order in favor of OFAC, upholding the $4 million civil penalty imposed by OFAC in 2014.

Lesson 2: Actual delivery of goods to Iran is not required

Epsilon appealed its $4 million penalties and the U.S. Court of Appeals for the District of Columbia affirmed in part and reversed in part the D.C. District Court's order.

One of Epsilon's arguments during the appeal was that Regulation31 CFR § 560.204, relating to transshipments to Iran, could not be violated when there was no actual export to Iran.

The majority of the Appeals Court did not agree, and said that the actual delivery of U.S. origin products to Iran is not required for the regulation to be violated. Instead, it held that the regulations restrict a U.S. exporter at the point of shipment from the U.S. where that exporter knows or should know that a third country specifically intends to re-export the goods to Iran, regardless of whether the goods ultimately arrive in Iran.

Lesson 3: ITRS Transshipment regulation is not a strict liability provision

Another take away from the Appeals court case is the acknowledgement that Regulation 31 CFR § 560.204, unlike several other OFAC regulations, does not impose "strict liability".

The transshipment regulation rather prohibits U.S. persons from exporting "goods, technology or services to Iran", including exports to third countries with "knowledge or reason to know" that the exports "intended specifically" for a shipment to be sent to Iran.

Nevertheless, according to the 2002 OFAC "Guidance on Transshipments with Iran", reasonable care must be taken to ensure that exports to third countries are not specifically intended for Iran and that third-country customers do not deal exclusively or predominantly with Iran. Therefore, while an exporter may satisfy themselves that its exports to a third country are not specifically intended for Iran, some due diligence is required to demonstrate the exporter had no "reason to know" that a customer was exclusively or predominantly doing business with Iran.

In this case, the Circuit Court upheld the OFAC determination that the transshipment provision could be triggered where substantial evidence (including website materials from Epsilon and the customer) supported a conclusion that, during one period of time, all of the relevant third-country customer's sales were to Iran.

The Appeals Court sent the case back to the lower court, with instructions to remand the case to OFAC for further consideration.

Lesson 4: Having no OFAC Compliance Program at the time of the violations is an aggravating factor

On September 13, 2018, OFAC issued the final settlement in the matter. The reduced September 2018 settlement amount reflects OFAC's consideration of the case, "in light of the D.C. Circuit's decision and pursuant to the General Factors under OFAC's Economic Sanctions Enforcement Guidelines."

OFAC mentions the following to be aggravating factors:

1. the Alleged Violations constituted or resulted in a systematic pattern of conduct;
2. Epsilon exported goods valued at $2,823,000 or more; and
3. Epsilon had no compliance program at the time of the Alleged Violations.

OFAC considered the following to be mitigating factors:

1. Epsilon has not received a Penalty Notice or a Finding of Violation in the five years preceding the transactions that gave rise to the Alleged Violations;
2. Epsilon is a small business; and
3. Epsilon provided some cooperation to OFAC, including entering into an agreement to toll the statute of limitations for one year.

OFAC also notes that, following litigation of the Alleged Violations, Epsilon took additional remedial actions to address the conduct that led to the

Alleged Violations, including terminating its relationship with Asra International and instituting an OFAC sanctions compliance program.

Summary

- The essential features of a sanctions compliance system include
  - Management commitment
  - Risk assessment
  - Organizational structure and internal controls
  - Testing and Audit
  - Training
- Management commitment is essential to the successful operation of the system
- A risk assessment identifies the ways in which an organization may be exposed to possible sanctions violations
- The compliance system should be designed to mitigate the risks identified in the risk assessment, resulting in full adherence to the law
- An effective sanctions compliance system requires an organizational structure that reflects and addresses the sanctions risks
  - The sanctions compliance function must receive adequate resources and have the authority to act when required
- Internal controls include an overall sanctions policy, as well as procedures addressing a variety of areas, including
  - Screening customers
  - Reviewing and approving transactions
  - Investigating possible violations
  - Reporting to management
- The operation of the system should be subject to periodic review and testing, either by the internal audit function or by an external auditor
- All employees, including senior management, should receive the training necessary to educate them regarding their responsibilities for sanctions compliance

Review Questions

1. What is the role of senior management in sanctions compliance?
2. What is the purpose of a sanctions risk assessment?
3. Who should issue the organization's general sanctions policy?
4. Name five procedures organizations should have to implement their sanctions responsibilities.
5. What is the role of audit in the sanctions compliance process?
6. Name three risks faced by financial institutions.

ROLE OF TECHNOLOGY AND LIST SCREENING

Association of Certified Sanctions Specialists (ACSS)
7950 NW 53rd Street Suite 337
Miami, FL 33166
Phone: +1 305 433 7187
helpdesk@sanctionsassociation.org
www.sanctionsassociation.org

Sanctions Screening: An Introduction

{T}ransaction screening is the most critical element of an internal compliance programme.

Draft EU Guidance on Best Practices for Internal Compliance Programmes

"Screening" in general refers to any sort of review of information regarding a person or transaction to determine if sanctioned elements are present. More technically, screening is the review of information for sanctioned elements by comparing the information to a list of names or terms. In the sanctions context, screening is the comparison of one string of text against another to detect similarities which would suggest a possible match. The purpose of sanctions screening is to detect and prevent sanctions violations by identifying locations, parties, or dealings potentially subject to sanctions. Typically, screening occurs by comparing words in a document, such as a bank payment message or a purchase order against a list of names of sanctioned individuals, entities, and countries. Screening may be conducted manually, although it is more typically performed electronically.

While not technically required by law, screening is an integral part of any sanctions compliance system. The FFIEC BSA/AML Examination Manual states flatly that, with respect to U.S. banks, sanctions compliance systems should include screening. Screening is not restricted to banks, though; any organization that does business internationally and has any exposure to sanctions should employ some sort of screening method. In this context, screening simply means knowing who your customers are; knowing the other parties to transactions; and knowing the destination of any products you're selling.

As with other aspects of a compliance system, screening should reflect the organization's risk profile, as well as its risk appetite. **The Wolfsberg Guidance on Sanctions Screening** enunciates the following core principles as the basis for the design and implementation of sanctions screening systems:

1. Articulate the specific sanctions risk the organization is trying to prevent or detect within its products, services and operations.
2. Identify and evaluate the inherent potential exposure to sanctions risk presented by the FI's products, services and customer relationships.
3. Develop a well-documented understanding of the risks and how they are managed through the set-up and calibration of the screening tool.
4. Assess where, within the organization, the information is available in a format conducive to screening.

In applying these principles, several factors that may affect the design of the screening system are:

1. The jurisdictions where the organization is located, which determines the sanctions laws that apply
2. The proximity of the organization - geographically, culturally and historically - to countries subject to broad sanctions
3. The organization's customers or clients, including
   a. Whether they international or domestic
   b. If international, where they are located; and
   c. What their business is
4. The volume of transactions
5. The complexity of transactions, including the distribution channels used
6. What products and services the organization offers and whether those products reflect a heightened risk of sanctions violations
7. The organization's business processes, and in particular, how it sells and delivers products

The objective of this process is to adopt a screening program that mitigates sanctions risks in the most efficient manner possible. The system may involve a significant investment in technology and require the services of tens or even hundreds of personnel, or it may be as simple as someone in Export Processing manually reviewing a purchase order. Whatever the system is, though, it must effectively mitigate the sanctions risks identified by the organization's sanctions risk assessment.

The Screening Process

While the mechanics of screening can be complicated, at heart the process is relatively simple and straightforward:

1. An organization receives information (usually in the form of some sort of message or document) relevant to its business. Such documents typically involve a customer, business relation, counterparty, transaction, or all of these. Examples of the types of information subject to screening include customer acceptance forms, contracts, purchase orders, invoices, and shipping documents. For financial institutions, this information is typically contained in various types of payment messages, although customer applications and data are also important.
2. The organization identifies what types of information need to be screened. These may include the names of customers, business partners, employees, or any party to a transaction. Information to be screened will also normally include the addresses of the parties involved, as well as the origin and destination of any physical shipments. It may even include information like ship names and, for manufacturing and trading companies, a description of the goods involved, including their country of origin.

3. The screening system (which may be automated or simply a person working from a written procedure) extracts the relevant information (the customer name, address, etc.) in the document and compares it to a list. The list will contain the names of individuals, entities, organizations, vessels, governments, and countries subject to sanctions. The subject of lists is discussed in detail below.
4. If there is a potential match between words in the document (such as a name) and words on a list, the system generates an alert. As the Wolfsberg Guidance on Sanctions Screening notes, "The generation of an alert as a result of the process of screening is not, by itself, an indication of sanctions risk. It is the first step towards detecting a risk of sanctions exposure, which can be confirmed or discounted with additional information to evaluate whether the similarities in the text reveal a true sanctions match."
5. The responsible person examines the alert to determine whether it is clearly not in fact an actual match, i.e., a false positive. If the word "Cuba" is included in the list against which terms are compared, for example, the word "scuba" might generate an alert. Another example would be Havana Café in Amsterdam.
6. If the reviewer decides that the alert is not a false positive, they may either forward it to someone else for further investigation or examine it further themselves to determine whether there is an actual hit. Who investigates at this point depends upon the particulars of the screening system. This further investigation may require obtaining more information – for example, the name, birth date, and passport number of a customer whose name matched a name on the list.
7. If the reviewer confirms that the match is an actual match – that the name in the document is the same person as a name on a sanctions list – the system generates a "true hit." At this stage, a second person may review the information to confirm the conclusion. This is known as the "four eyes principle."
8. If the reviewer(s) confirm that there is a true hit, some sort of action is required. Depending upon the relevant sanctions or company policy, this action could include declining to perform the transaction, rejecting the transaction, or freezing the funds.

While the process of screening is relatively simple, the actual application can be quite complex. Among the issues the screening system must address are:

1. What lists are to be screened against?
2. How does your system identify possible matches?
3. What is the process for reviewing alerts and determining whether they represent true hits?

Lists and List Management

Official Lists

As the above discussion indicates, lists lie at the heart of the screening process. The selection of which lists against which information will be screened determines what customers and transactions may be allowed, and which must be rejected. The lists organizations must screen against depends in the first instance on where they are located. Organizations and individuals must comply with the laws of their home country. This means that, if their home country has a list of individuals and entities against whom sanctions apply, screening should be against that list. Both the EU and the United States have such lists – the EU Consolidated List and the U.S SDN List respectively. In addition, the United States also maintains other lists, including the Sectoral Sanctions Identifications List. All non-SDN lists are included in OFAC's Consolidated List.

Organizations may also screen against lists of other institutions and countries. Organizations doing business in U.S. dollars will typically screen against the U.S. SDN and Consolidated Lists, to assure that any transactions flowing through the United States are not rejected or frozen. Similarly, organizations who do business in the European Union may screen against the EU lists, even if they do not have actual subsidiaries in the EU. The same will be true with respect to any other country with its own list. In this respect, it is important to remember that many EU members have their own sanctions lists in addition to the EU list. While the country-specific lists may have only a few additional names, it is important to keep them in mind as well. Finally, many organizations choose to screen against the UN list to ensure that they are not doing business with any entity or individual subject to UN sanctions, whether or not those sanctions are incorporated into their home country's sanctions list.

Sanctions lists are not necessarily the only lists against which organizations will decide to screen, though. Countries may maintain other lists of individuals and organizations against which other restrictions apply. In the United States, for example, Bureau of Industry and Security, which administers export controls, maintains the denied persons list of persons who may not export from the United States, and the entity list of foreign parties that are prohibited from receiving imports from the United States. The U.S. State Department maintains a list of individuals and entities subject to nonproliferation sanctions, as well as the AECA list of parties who are prohibited from participating in the exportation of defense articles. All of these lists, including the OFAC lists, are combined in a single consolidated U.S. sanctions list, which is available at https://www.export.gov/csl-search. Similar lists may be available in other countries. By screening against all of these lists, organizations ensure that they do not run into obstacles in transactions.

Internal Lists

Organizations may also maintain their own internal lists. These are typically described as "good guy" and "bad guy or grey" lists.

"Good guy" or "white" lists include names that have been screened and confirmed not to represent a true hit. This may occur, for example, if a customer has the same name as someone on a sanctions list.

"Bad guys" or "grey" lists reflect the opposite. These are individuals or entities whom the organization has determined have ties to sanctioned or other financial crime-related parties, even if they are not sanctioned themselves. They may present a financial crime risk to the organization, and have been identified through the organization's internal procedures or intelligence. The names are generated and maintained within the organization's risk appetite and, ideally, applied in screening for a set time frame, depending on the risk. Organizations may decide not to do business with these "bad guys" as a matter of principle, even if it may be technically legal (for the time being at least) to do so.

Sources of Lists

There are many different sources of lists. Organizations can simply rely on the official list, which is typically available online. However, if the organization is screening electronically, this may require the organization to import the revised list and incorporate it into its screening every time there is a change. Most more sophisticated organizations, though, use commercial vendors. The advantage of this is that the vendors automatically update their lists. Typically, the service includes updating the list inside the user's system automatically. This is also a way to access multiple lists across jurisdictions, without having to monitor each continually and download changed lists into the screening system.

What to Screen?

An obvious question is exactly what is the organization going to screen? At the least, organizations should screen customers, other business partners, employees, and transactions. Exactly what information is screened, and how the process occurs, may vary.

Customer and Business Partner Due Diligence

Organizations should screen customers and business partners, such as suppliers. Most organizations already do; "screening" occurs whenever an organization decided whether to accept a new customer or take on a new supplier. With customer and business partner due diligence, though, the mechanical screening against sanctions lists is only part of the process.

The information to be screened with customers and business partners starts, of course, with the name. However, it is advisable to screen other information as well, especially the address. This will indicate whether the customer or business partner is in a country subject to sanctions. While they may not be screened, information on customers and business relations should, for individuals, include additional identifying information, such as birthdates and passport numbers. This will allow the organization to confirm that the customer or business partner is not in fact subject to sanctions, should there be an initial match.

While screening the names of individuals may seem straightforward, there is a complication. People have the same names, especially in some regions. To screen accurately, an organization will often require more than just the name of the potential customer or business partner. Additional information that will allow the organization to screen the name accurately includes address, birthdate, and passport number. Some organizations, such as banks, collect this information as a matter of routine.

As discussed earlier, entities that are owned or controlled by sanctioned parties may themselves be subject to sanctions, whether they are separately designated or not. This means that it is necessary to determine the “ultimate beneficial ownership” of the entity. This goes beyond simply who the obvious owners are; the ultimate beneficial owners (UBOs) are the individuals who own the entity when all the lines of ownership are followed. To accomplish this, the organization must request information on UBOs at the time the customer or business partner is on-boarded.

Obviously, many entities have many – even thousands – of owners. For this reason, organizations typically request information only on owners with more than a designated share of the entity. The most commonly used figure is 25 percent, although banks in particular may request UBO ownership all the way down to the 10 percent level. The organization must then screen the names of the UBOs, as well as the names of all other entities in the ownership chain, against the applicable sanctions and other lists. If an entity is itself owned by two entities, and each of those has two UBOs, the organization would screen five names in total.

Ownership changes. The acquisition of ownership in an entity by a party subject to sanctions after the entity has already been screened could put the organization in the position of doing business with a sanctioned party without its knowledge. For this reason, organizations require notification if any new party acquires more than the designated percentage of the entity.

As this discussion shows, having accurate information on ownership is essential to the effective screening of customers and business partners. A refusal of an entity to provide ownership information is a red flag. If a potential customer or business partner will not provide its UBOs, or provides only partial information, the organization should investigate further. If it cannot obtain the necessary information, it should protect itself by declining to do business with the entity.

Employee Screening

Organizations should also screen their employees, especially if they operate internationally. The information that should be screened is the same as for customers.

Transaction Screening

Organizations should screen at least some of their transactions. Which transactions to screen depends upon the risk profile. A company could choose, for example, to screen only international transactions. It may also screen any transactions in a particular currency, such as U.S. dollars. Finally, it should screen any transaction that involves the cross-border delivery of goods, services, or technology, even if the customer is domestic.

Deciding which information to screen regarding a transaction is a major issue. Unlike customers, where the amount of information is relatively limited, an individual transaction may generate multiple documents and contain information not necessarily relevant to determining whether a sanctioned element may be present. An organization should initially assess which transaction types are relevant for sanctions screening. It should then identify which attributes within those records are relevant for sanctions screening. Names of parties involved in the transaction are relevant for list based sanctions programs, while addresses are more relevant to screening against country sanctions. Addresses can be used as identifying information to help distinguish a true match from a false match. Other data elements, such as ports, vessel names, and bank identification codes may be relevant for both list and geographically based sanctions. Finally, specialized transactions, such as securities transaction, may involve information such as International Security Identification Numbers (ISIN) that can be useful in identifying potentially sanctioned transactions.

In a sanctions context, some data elements are more relevant when found in combination with other attributes or references. For example, detection of sectoral sanctions risk typically requires detection of multiple factors, such as those where both the targeted parties and the prohibited activities are involved. On the other hand, information such as invoice or reference numbers, dates, and amounts may be less useful in identifying sanctioned elements in a transaction.

The Wolfsberg guidance on sanctions screening by banks notes that the following are some of the data elements in transactions that are most commonly screened. While the Wolfsberg guidance is specifically for banks, many of these suggestions are relevant to other types of organizations as well:

1. The parties involved in a transaction
2. Agents and intermediaries
3. Vessels, including International Maritime Organization (IMO) numbers

4. Bank names, Bank Identifier Code (BIC) and other routing codes
5. Free text fields, such as payment reference information or the stated purpose of the payment in Field 70 of a SWIFT message
6. International Securities Identification Number (ISINs) or other risk relevant product identifiers, including those that relate to Sectoral Sanctions Identifications8 within securities related transactions
7. Trade finance documentation, including the:
8. Importer and exporter, manufacturer, drawee, drawer, notify party, signatories
9. Shipping companies, freight forwarders
10. Facilitators, such as insurance companies, agents and brokers
11. FIs, including Issuing / Advising / Confirming / Negotiating / Claiming / Collecting / Reimbursing / Guarantor Banks
12. Geography, including a multitude of addresses, countries, cities, towns, regions, ports, airports, such as:
13. Within SWIFT Fields 50 and 59
14. Place of taking in Charge / Place of Receipt / Place of Dispatch / Place of Delivery / Place of Final Destination
15. Country of origin of the goods /services / country of destination / country of transshipment
16. Airport of Departure / Destination

Technical Issues

Screening involves several technical issues. These include the methodology for matching (including sensitivity); rules for suppressing hits; and timing of screening.

Matching Methodology

The bank's policies, procedures, and processes should address how the bank identifies and reviews transactions and accounts for possible sanctions violations. For screening purposes, the organization should clearly define its criteria for comparing names provided on the sanctions lists 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 hit is a valid match or a false hit.

An initial issue is what the organization is screening against. Lists do not contain just "a" name. There may be variants, as well as strong and weak aliases. Furthermore, because of differences in alphabets, the same name may be spelled different ways in different places. The organization's screening procedures must take these facts into account by providing, for example, whether screening is against weak as well as strong aliases. Further, to keep sanctions evaders from fooling the system, the matching methodology must take into account misspellings, common variations, and tricks evaders have tried to use to fool matching algorithms, such as by inserting spaces or characters inside a name. This is especially true if, as banks do, screening is done electronically rather than manually.

The short term for considering all of these factors is "sensitivity." How sensitive is the system to a near-match? A system that requires a 100 percent match – that the name in the record being screened match exactly the name on a list – risks letting matches through because of insignificant differences. Requiring only a weak match, on the other hand, can flood the system with false positives, taking time away from investigating more complex cases.

There is no perfect answer, and the precise matching methodology should reflect the organization's risk assessment.

Case Study "Beyond Stripping": National Bank of Pakistan

In June 2015, the National Bank of Pakistan paid a $28,800 penalty to US Treasury for apparent violations of US sanctions programs. Unlike "stripping cases", in this instance, the filters were not manually tricked, but failed to catch illicit transactions because of technical flaws. In fact, according to Treasury, the prohibited transactions were mistakenly processed due to a software failure. Violations of sanctions laws were enforced so strictly that the institution was punished anyway.

OFAC stated that the New York branch of the bank processed wire transfers totaling $55,952 for the sanctioned Kyrgyzstan airline, Kyrgyz Trans Avia. OFAC blacklisted Kyrgyz Trans Avia in 2013 after authorities alleged the airline helped Iran acquire aircraft which may have been used to deliver weapons for the war in Syria.

The bank's sanction screening tool failed to detect the name of the account name "LC Air company Kyrgyztransavia" as belonging to Kyrgyz Trans Avia account, OFAC said. This is an example of an occasion where a human would probably have recognized the match. The software, however, had not been programmed to consider alternatives where names were joined, so that the transaction was mistakenly allowed.

The following article from www.sanctionsassociation.org explains pitfalls for financial institutions in sanctions screenings.

For financial institutions, sanctions compliance is complex and fraught with risk

March 24, 2016
By Debra Geister of Section 2 FIS

For many banks, and indeed for other business organizations, undertaking a sanctions compliance program seems at first like a straightforward, relatively easy endeavor. After all, how difficult can matching names be?

It is true that of the operational areas a bank has to confront in anti-money laundering (AML) compliance, economic sanctions is one of the less complex ones. However, it is not as easy as it looks. As many financial institutions will acknowledge, managing sanctions compliance can be confusing and challenging and always high-risk.

Lack of a single solution makes field challenging, complicated

What makes it so challenging and complicated to manage? The primary reason is that as in many compliance functions, no single solution fits every business. Each program must be specifically tailored to the particular type of business and operation. If the business operates in multiple countries, there can be overlap and conflict. In addition, sanctions lists are intrinsically challenging because many names are common and come with limited additional information to ascertain true matches.

For example, a person named Charles Taylor is under review. He may be on a Politically Exposed Person list, meaning he is a public official or close associate of the official in another country. In most such cases, date of birth, street address and other information is limited or unavailable. Charles Taylor is not an uncommon name in the US so a “hit” may generate many false positives that require review. With little information to disqualify the false positives at the start, the hits would create an operational burden for the operations team. Combine this “common name problem” with the fact that a Charles Taylor is on the OFAC list. The complicating factors that arise become clear, constituting the factors and challenges that make sanctions compliance anything but simple and straightforward.

Constructing a sanctions compliance program includes several factors. They include the type of business conducted, location of the business, whether it exports goods and services across borders and, of course, what the organization’s appetite for risk is. For businesses located in the United States, the sanctions compliance program can be fairly clear. Compliance with the regulations of the Office of Foreign Assets Control (OFAC) is mandatory and, without exception, a program must be constructed and implemented. OFAC requirements apply to everyone in the United States in all kinds of businesses.

Risk-based approach to compliance is the best route

In addition to OFAC's list of "Specially Designated Nationals" (SDNs), lists maintained or derived from the requirements of other government agencies must also be considered, including lists of Politically Exposed Persons and other enforcement lists of various agencies. The Arms Expo Control Act (AECA) and the "Debarred" lists of the US State Department are examples. The U.S. Departments of State, Commerce and Treasury determine that entries on their respective lists are a potential threat to domestic export control requirements and "Denied Persons" list of the U.S. Commerce Department's Bureau of Industry and Security (BIS). BIS targets companies that export goods from the US. Its lists must be reviewed to see if they apply to a business. For a financial services institution, OFAC compliance in large measure depends on the geographic scope and nature of the business customer and who its customers are. As with many areas of financial and business regulation, the answer is usually found in a risk-based approach.

For businesses outside the financial services arena, pinpointing the lists that merit priority can be difficult, but a risk assessment based on factors such as geography, export activity, type of products and customers usually leads to the right compliance decision. Several best practices, guides and questions should be kept in mind:

Key questions that test sufficiency of compliance program

1. Are the operational, risk and legal teams synchronized and collaborating?

- Sanctions program decisions should be a joint effort. None of the teams in an organization can effectively perform its job or make decisions without considering what the other team is doing.
- Give due weight to the significant risk faced by the organization if operational procedures are not aligned with the overriding policies.
- It may be easy to write a policy, but putting it into operation is often difficult, especially if there are conflicting views or a lack of good communication among the teams.
- Controls, such as the settings of the filtering software and false positive rules, should be consistent with the policy standards. Are the standards reflected in the procedures? Do they clearly reflect the risk-based approach of the organization?
- The risk and legal teams must sufficiently understand the operational process so they make informed decisions and provide proper guidance. The effects on the organization of a policy decision must be considered before, not after, a program is implemented.
    - If, for example, the legal team decides the Australian National Security's terrorist organization list must be screened, it should

provide direction on how to handle a match before list implementation begins. Must a match be reported to a regulatory agency? Are there reporting timeframes? Should the organization end its relationship with the matching party or only conduct "enhanced monitoring"? Is enhanced monitoring defined? What is the escalation process for final decisions? Collaboration is critical in making operational decisions that support the objectives specified in the organization's policies.

2. What identifying information is available to determine matches?

- A financial institution likely has four data points of its Customer Identification Program or CIP: name, address, date of birth (DOB) and identification number. All of them help to prove or disprove name matches, but that is only part of the task.
- If additional data points are not gathered, can the organization start gathering them for future screening? Aside from name, DOB or age is by far the most valuable information to help with OFAC and other alert clearing. It is no accident that the great investigative agencies, such as the Federal Bureau of Investigation, New Scotland Yard and IRS Criminal Investigation, consider date of birth one of the crucial facts in pinpointing a person's identity. Depending on circumstances, adding a date of birth filter can reduce false positive reviews by 50 to 90%.

3. Has proper attention been given to the research tools that help with alert clearing?

- The less information that exists about a party, the more likely it is that an outside information source is required. Free open sources, such as Google or Personlookup.com, may provide missing data about a party. Otherwise, the organization should consider purchasing research tools from existing providers.
- Each list against which screening is conducted may require a different research source and distinct operational procedures.

It is crucial to understand internal risk, strategy

There are no easy answers to the questions the organization, including the legal team, may have. There is no help hotline for questions about the requirements of lists that jurisdictions publish. Much time may be required to find necessary information. Often, vendors will suggest that multiple new lists should be maintained. More lists are not necessarily the answer. Instead, a good understanding of the organization's risk and strategy and a determination of how, or if, additional lists are consistent with the risk and strategy are key first steps.

The organization should understand the operational impact and risk of adding sanctions lists. The approach that "more lists are better" is a fallacy. If more lists bring resource constraints and the organization is not prepared to handle them, risk can increase. Taking on new operational burdens can be more detrimental than not including a list in the program. In addition to analyzing the impact, the new lists should be reviewed for risk and strategic fit. By understanding the impact of these factors, the organization's oversight and operations teams can plan a successful launch of added sanctions lists and remember that:

- Difficulties arise in navigating and understanding sanctions lists and their regulatory applicability when websites are in a foreign language, as is often the case,
- Vendors offer watch lists to their corporate customers without providing details of the entities on the lists or of the source of the lists,
- Guidance provided at compliance forums is often very limited. For example, the ACAMS forum posts inquiries from compliance officers who ask for global sanctions guidance, but the responses are slim. Risk versus cost should be weighed when considering additional lists.
- It may sound like a simple solution to take a risk-averse approach and screen all sanctions and enforcement lists, but remember that the organization's costs rise with each list, especially global lists. Building a process to handle each type of alert and match is not quick, easy or inexpensive.
- In the U.S., it takes an analyst up to five times as long to clear an alert for a non-U.S. party than for a U.S. party, depending on the operational plan and availability of data.
- It can be onerous to stay abreast of regulatory changes in U.S. sanctions programs. Consider the maintenance required to screen for the sanctions programs of multiple countries. Is it advisable to review list applicability and changes in regulatory direction annually or to try to stay abreast of updates throughout the year?
- Many sanctions lists contain the same entities. Determining match risk mitigation strategies addresses this possibility. The testing process should highlight this crossover and the impact on operations.

Compliance is a major mission and failure leads to risks, possible calamities

There are many operational facets of sanctions compliance management. Sanctions compliance is a major undertaking and failures can lead to compliance, legal, reputational, criminal and operational risks and calamities. Inadequate sanctions compliance can lead to civil money penalties, criminal prosecution and regulatory consequences. U.S. regulators are the most active of all global agencies in levying money penalties and pursuing actions against entities worldwide. U.S. sanctions agencies, such as OFAC, have levied billions of dollars in penalties against organizations, as in these examples:

- 20, 2015 – Crédit Agricole Corporate and Investment Bank was penalized by OFAC for more than $1 billion, mainly for sanction violations. https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20151020_cacib.pdf

- March 12, 2015 – Commerzbank AG suffered OFAC money penalties and forfeiture of $1.45 billion. The penalty was part of a global settlement among Commerzbank, OFAC, the U.S. Department of Justice, the New York County District Attorney's Office, the Federal Reserve Board of Governors, and the New York Department of Financial Services. Sanctions violations came from 1,596 transactions with SDNs and with U.S.-sanctioned nations, Burma, Cuba, Iran, and Sudan. https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20150312_commerzbank.pdf
- The U.S. sanctions-related laws and regulations are by far the most actively enforced and create the highest standards for sanctions compliance and enforcement. Anyone that does business in the U.S. should be diligent about their sanctions compliance program.

Summary

Sanctions laws and regulations have wide applicability and impact all businesses. Global sanctions apply not only to banks but to any company that does business abroad. Thus, the need for global sanctions compliance is expansive. In view of this great impact, a thorough sanctions program can help a business avoid regulatory, legal and reputational problems.

Businesses must have a clear and consistent risk assessment program to determine the sanctions risks. They should apply risk assessments comprehensively. The operations team should create policy-driven procedures that address all global risks and operations. Adding more lists to a program is not always a sound path. Following these steps may ensure the existence of a good sanctions program.

Important Terms

The Wolfsberg Screening Guidance provides several key definitions related to screening:

Fuzzy Matching is a varied and algorithm based technique to match one name (a string of words), where the contents of the information being screened is not identical, but its spelling, pattern or sound is a close match to the contents contained on a list used for screening.

Customer or Name Screening is the screening of full legal name and any other name provided by the customer, such as known aliases, against applicable official sanctions lists.

Transaction Screening is the process of screening a movement of value within the FI's records, including funds, goods or assets, between parties or accounts. In order to mitigate risk associated with trade finance transactions and international wire transfers, FIs conduct real-time screening of crossborder transactions against Sanctions Lists, where any of the Sending Bank, Originating Bank, Receiving Bank, Intermediary Bank or Beneficiary Bank are located in different countries.

Alert Spike is a substantial increase in the number of alerts generated. A spike could be caused by, for example, remediation exercises, changes or updates to policies, procedures or Watchlists.

True Match is a screening result, where the characters contained within the information being screened match the details of a designated entity on a list that is in scope for screening.

Weak Aliases/Low Quality Aliases is a term for a relatively broad or generic alias (including 'nicknames' and common acronyms) that may generate a large volume of false hits when such names are run through a computer-based screening system. It is not expected, nor is it typically productive, to screen against weak aliases.

Rules

Related to sensitivity is the question of rules. These are typically pieces of code that instruct the matching algorithm to ignore matches under certain circumstances. The rule could be as simple as "ignore matches for John Q. Smith," or they can be quite complicated. Rules should be constantly tested against the system to ensure that they are not resulting in ignoring probable true matches.

Timing of Screening

The timing of screening is another key issue. Transactions are normally screened in real time, before they are executed. If there are a very large number of transactions of a certain type, though, or if the risk of a sanctions violation is small, it may be more efficient to use batch screening, i.e., screening all transactions of a given type at one time.

Customer and business relation names present a more difficult problem. Obviously, these should be screened before the customer is accepted or the business relationship established. Customers or business partner could be placed on a sanctions list after they have been accepted, though. Does the organization re-screen its entire customer base every time a list changes, or only at set intervals? Again, this depends upon the organization's risk profile, as well as the resources available for screening.

Another type of screening is event-driven screening. This refers to screening that occurs in response to adverse news about a customer, for example. Integrating event-driven screening into the overall system requires some sort of method for monitoring relevant news and creating a link between that news and the screening tool.

Screening Tools

As this discussion indicates, the creation of a screening system can be a complicated and expensive process. For this reason, many organizations purchase screening solutions from vendors. These solutions can be customized to reflect the organization's precise needs, but usually contain certain standard components. This eliminates the need for the organization to build the entire system from scratch. On the other hand, these systems can be expensive, and it is important that they reflect the organization's risk factors and needs.

Alert and Hit Handling

A fundamental issue in any screening system is how alerts (possible matches) and hits (actual matches) are handled. As noted above, the first step in the screening process is for an individual to review an alert generated by the system (whether automatically or manually) to assess whether it is obviously a false positive. The question is what happens after that? The first alternative is to have the same person investigate the alert further to determine whether it is an actual hit. Another alternative is to have the same person do just enough of an investigation to determine whether there is a potential hit, and then turn the investigation over to a specialized function. The final common alternative is for one person to review the initial alert; if they cannot dismiss it, they turn the matter over to someone else whose function is specifically to investigate potential hits.

A related issue is how many people are required to confirm that a hit is a true hit. Assessing a hit as "true" has potentially significant implications. At the least, it may require the rejection of a transaction, with possible harm to the customer and other parties involved. At most, it may require the freezing of property. Given this, the question is whether one person should be able to classify a hit as true, or whether a second opinion is required. That second opinion typically comes from someone in the compliance function who has received special training. This second alternative, requiring at least two people to assess the hit, is called the four eyes principle, and is common in sophisticated screening systems, such as at large international banks, where the potential harm from classifying a hit incorrectly can be substantial.

KPIs, Testing, and Audit

To ensure that the screening system is functioning adequately, it is necessary to gather information about the operation of the system on a regular basis. This allows management to detect shortcomings and to correct inefficiencies. Typical Key Performance Indicators of sanctions screening systems include

- The number of transactions screened
- The number and percentage of alerts generated
- The number and percentage of true hits
- The ratio of true hits to alerts
- The average time for investigating an alert
- The average time for investigating a true hit
- The number and percentage of cases left open after a specified period, such as 24 or 72 hours

As with all other aspects of a sanctions compliance system, the screening system should be subject to periodic testing and audit.

Recommended Functions within a Screening System

The BSA/AML manual, the New York DFS regulations, and various OFAC penalty notices have identified a number of features and functions that should be included in a sanctions screening system, reflecting many of the points made above. The following list summarizes the key characteristics of an effective sanctions screening system:

- A system for screening transactions and customers for possible sanctions exposure
- The bank's filtering system for transactions and customers is based on technology, processes or tools for matching names and accounts, in each case based on the institution’s particular risks, transaction and product profiles
- All data sources that contain data relevant for screening and monitoring have been identified
- The relevant systems are subject to on-going analysis to assess the logic and performance of the technology or tools for matching names and accounts, as well as the relevant sanctions lists and the threshold settings to see if they continue to map to the risks of the institution;
- There is documentation that articulates the intent and design of the Filtering Program tools, processes or technology
- Qualified personnel or outside consultant(s) ae responsible for the design, planning, implementation, operation, testing, validation, and on-going analysis of the Transaction Monitoring and Filtering Program, including automated systems if applicable, as well as case management, review and decision making with respect to generated alerts and potential filing
- There is a formal vendor selection process if a third party vendor is used to acquire, install, implement, or test the Transaction Monitoring and Filtering Program or any aspect of it
- Customer names are screened before the customer is accepted
- A policy for periodically screening existing customers

- Screening in real time, as opposed to batch screening
- A policy re what types of transactions (and, for banks, message types) will be screened
- A policy re transactions that are not screened A policy re screening domestic transactions
- A policy re screening international payments
- Data extraction and loading processes that ensure a complete and accurate transfer of data from its source to automated monitoring and filtering systems
- Screening procedures that identify the criteria for comparing names and identifying sanctioned countries, including taking misspellings and variations into account
- A process for identifying naming variations and misspellings
- Procedures for identifying false positives (alert and hit handling)
- A process for setting name screening sensitivity
- A process for assessing volume of hits and false positives to determine whether the sensitivity of the system needs to be revised
- A process for identifying, incorporating, and updating lists used in screening
- A policy re including the names of cities in sanctioned countries in filters
- The incorporation of abbreviations in screening
- The inclusion of vessel names in lists
- A policy regarding a good guys list
- A procedure for identifying and screening a customer's location to identify whether customers may be located (temporarily) in sanctioned countries
- Screening software or methodology that accounts for hyphens, initials, and additional middle names in identifying potential matches
- Adequate funding is available to design, implement and maintain a Transaction Monitoring and Filtering Program that complies with the relevant requirements

Conversely, examples of deficiencies in the screening process, include:

- Insufficient capacity to assess alerts;
- Filtering criteria that are too loose, generating too many “false positives”;
- Filtering criteria that are too strict, potentially missing real hits (false negatives);
- Closing alerts without proper investigation due to back log;
- Excluding certain transactions from the filtering process without first assessing the risk this poses;
- The company has no access to older alerts that have already been investigated or closed;
- Watch list filtering is not carried out frequently and not clearly scheduled;
- Persons and entities on the suppression list are not screened periodically or when changes are made to the lists;
- No up-to-date sanctions lists are used.

Outsourcing

Precisely because it is highly technical and can be expensive, organizations may outsource screening to third parties. This can be an economically viable solution, and can increase accuracy, as the screening is carried out by a dedicated function that the organization might otherwise not be able to afford. It is vital, though, that the third party's methodology and resources reflect the needs of the customer, and in particular its risk assessment. While outsourcing of screening is not prohibited, regulators have made clear that the original organization, not the screening supplier, remains responsible for the ultimate effectiveness of the system.

Summary

- Screening is an essential aspect of sanctions compliance
- Screening refers to the comparison of information in a record to a list of individuals, entities, vessels, and geographic locations subject to sanctions
- Organizations should screen customers, business relations, employees, and transactions
- The methodology for screening should reflect the organization's risk assessment
- Customer and business relation screening should include screening beneficial ownership as well
- An organization's screening methodology should address
    - What is screened (customers, transactions)
    - When screening occurs
    - What lists are screened against
    - How alerts are handled

Review Questions

1. What is screening?
2. What is meant by "ultimate beneficial owner"?
3. At what point are transactions normally screened?
4. Name five issues a screening procedure should address.
5. What are the dangers of setting the screening filter to a high degree of sensitivity?
6. What are three KPIs for a screening system?

OPERATIONAL ISSUES CONTRIBUTING TO AN EFFECTIVE AND EFFICIENT SANCTIONS COMPLIANCE PROGRAM

Operational Issues: Introduction

Effective sanctions compliance involves a number of significant operational issues. These include

- Resolving standard and complex cases
- Obtaining, managing, or reviewing licenses
- Freezing property, and managing frozen property
- Using contractual clauses to mitigate sanctions risks
- Outsourcing compliance functions
- Record keeping

The operation of a sanctions compliance system frequently requires interaction with other areas of compliance, especially export controls, anti-money laundering, and anti-corruption. It also requires the compliance function to be aware of, and be prepared to address, forces from the business side that may make compliance with sanctions laws more difficult.

Resolving Cases

Much of sanctions compliance involves the design, implementation, and maintenance of various systems, such as screening. One of the most important of these "systems" is that for resolving cases. In most instances, such as when screening reveals the presence of a sanctioned party, the decision is clear – the transaction cannot proceed. In some cases, though, the outcome is less obvious. Sanctions may apply to a party, for example, but may not necessarily prohibit all transactions. In these instances, a decision by the compliance function as to whether the transaction can proceed may be necessary. Many of these cases are relatively straightforward. Some, however, can be quite complex.

"Standard" cases can typically be resolved within the compliance function. Depending upon the complexity of the issue, the person handling the initial alert may be able to make a decision. More complicated cases may require consultation with others in Compliance. Large banks and other organizations often have both local and group-level sanctions expertise, and especially complicated cases may require a referral to the group's experts.

Especially complicated cases may require even more expertise. At one level, such issues may involve detailed questions regarding the underlying business, such as specific goods or financial services. Understanding these details may well require discussions with the business. On another level, a complicated case may raise difficult legal questions. Answering these question my involve the organization's legal function. Especially difficult legal questions may even require consultation with outside counsel.

Some cases are complicated, not because of the issues involved, but because of their significance to the organization. A given transaction may be legal, but engaging in it could raise major issues of reputation. In such cases, senior management may have to make a decision as to whether and how to proceed. Of course, senior management should always act in full compliance with the law. An organization should have clear procedures describing how both standard and complex cases are addressed.

Another layer of complexity arises when there is internal conflict over the proper resolution of a case. The conflict is frequently between the business and the compliance function, although conflicts can occur even within compliance. In many such instances, both sides can marshal strong arguments for their position. The organization should have a procedure describing how such disputes are resolved, including the conditions under which senior management must make a decision.

Licenses

A license is an authorization from the relevant authority to engage in a transaction that otherwise would be prohibited. The ability to obtain and manage licenses is accordingly an important aspect of sanctions compliance.

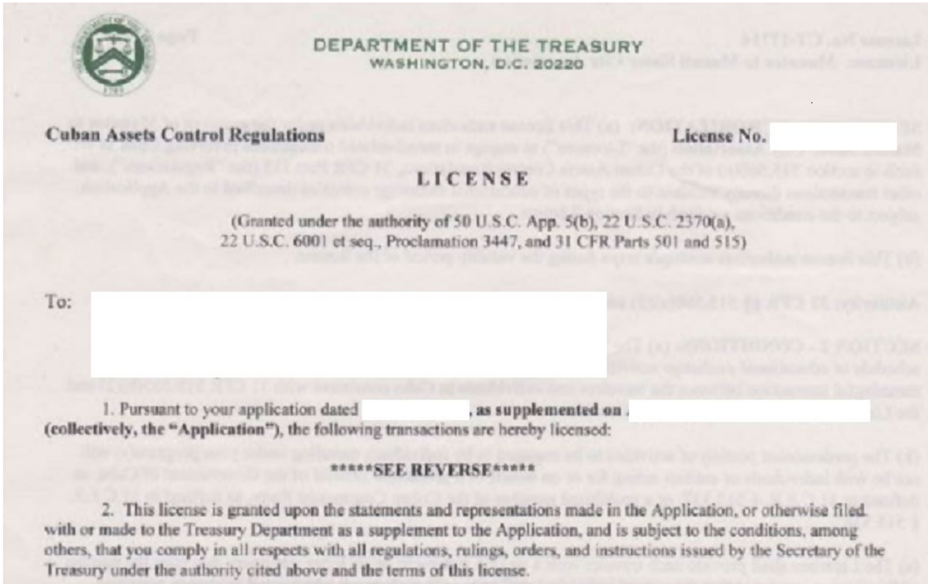
Types of Licenses

While details vary between countries, there are in general three types of "licenses."

An **exemption** states that the sanctions laws simply do not apply to certain conduct or types of transactions. No application or prior approval is required.

A **general license** authorizes a particular type of transaction that would otherwise be prohibited without the need to apply for a license. A general license may or may not limit its availability to a certain class of persons. Some U.S. general licenses, for example, may apply only to U.S. persons. A person may simply engage in the conduct authorized without prior approval, and often (though not always) without the need to file any reports. Of course, transactions must fall within the scope of the general license.

A **specific license** is a written authorization issued by the relevant authority to a particular person or entity, authorizing a particular transaction or series of transactions involving specified goods, services, or technology in response to a written license application. Persons engaging in transactions pursuant to a specific licenses must make sure that all conditions of the license are strictly observed.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Cuban Assets Control Regulations **License No.**

LICENSE

(Granted under the authority of 50 U.S.C. App. 5(b), 22 U.S.C. 2370(a), 22 U.S.C. 6001 et seq., Proclamation 3447, and 31 CFR Parts 501 and 515)

To:

1. Pursuant to your application dated , **as supplemented on** **(collectively, the "Application")**, the following transactions are hereby licensed:

*****SEE REVERSE*****

2. This license is granted upon the statements and representations made in the Application, or otherwise filed with or made to the Treasury Department as a supplement to the Application, and is subject to the conditions, among others, that you comply in all respects with all regulations, rulings, orders, and instructions issued by the Secretary of the Treasury under the authority cited above and the terms of this license.

License Applications

Who can apply for and grant a license, and the form of application, also vary between countries, and sometimes even between different licensing authorities within a country. Most license applications do not have to be submitted on a particular form. However, it is essential to include in the request all necessary information as required in the application guidelines or the regulations pertaining to the particular sanctions program. When applying for a license, it is always necessary to provide a detailed description of the proposed transaction, including:

- The identity of the party or country subject to sanctions that is the subject of the application
- The name and address of the applicant (whether the buyer, seller, or financial institution)
- The names of any entities that might perform services for or act on behalf of the applicant, including corporate affiliates, suppliers, and subcontractors
- A detailed description of the goods, services, or technology subject to the application
- Whether the license is sought for a single transaction, for multiple transactions, or for unlimited transactions over a given period of time
- The beginning and end date of the license

License Applications in the United States

In the United States, OFAC usually issues licenses to engage in transactions with parties subject to sanctions, although in some cases BIS or the State Department might be responsible instead. OFAC requires that applications be filed through its electronic system, which is available at https://licensing.ofac.treas.gov/Apply/Introduction.aspx. OFAC issues four general categories of licenses:

- Cuba travel
- Exports of agricultural and medical products to Iran or Sudan under the Trade Sanctions Reform and Export Enhancement Act of 2000 (TSRA)
- Release of blocked funds
- Specific license or interpretive guidance ("Transactional")

Depending upon the transaction, there may be specific guidance available on OFAC's website under relevant "Guidance on Licensing policy" on OFAC's various sanctions program web pages.

A license from OFAC may be necessary if there is any U.S. nexus with the proposed transaction. This includes

- Participation by U.S. persons, including citizens, companies, and financial institutions, in any role
- Participation of foreign entities owned or controlled by U.S. persons in transactions involving Cuba or Iran
- U.S. origin goods, technology, or services
- Use of U.S. dollars
- Use of information technology or other systems in the United States to process the transaction, even if no U.S. person is directly involved in the transaction

No license from OFAC is necessary if

- The activity is not subject to sanctions at all, such as travel by U.S. persons to Iran
- The activity is subject to an exemption, such as the import or export of informational materials, mail, or telecommunications
- A general license applies
- A license is necessary, but the relevant licensing authority is BIS or DDTC rather than OFAC

In some cases, a license from both OFAC and either BIS or DDTC may be necessary:

- Transactions involving Crimea
- Exports to SDNs in Cuba, North Korea, or Syria

Applicants may increase their chances of receiving a favorable determination by

- Providing a full explanation of the transaction, including the goods, services, or technology involved and a discussion of why granting the license is consistent with the goals of the relevant sanctions program

- Calling the OFAC Licensing Hotline in advance to obtain guidance
- Reaching out to the licensing officer, once one is assigned, and encouraging them to ask if they need additional information
- Requesting expedited treatment only if truly necessary

Many of OFAC's licensing determinations are guided by U.S. foreign policy and national security concerns. Numerous issues often must be coordinated with the U.S. Department of State and other government agencies, such as the U.S. Department of Commerce. Please note that the need to comply with other provisions of 31 C.F.R. chapter V, and with other applicable provisions of law, including any aviation, financial, or trade requirements of agencies other than the Department of Treasury's Office of Foreign Assets Control. Such requirements include the Export Administration Regulations, 15 C.F.R. Parts 730 et seq., administered by the Department of Commerce, and the International Traffic in Arms Regulations, 22 C.F.R. Parts 120-130, administered by the Department of State.

OFAC often takes months to respond to even fairly routine license requests. Even a request for a TSRA license may take 30 days or more. Response times for most transactional applications range from 9 to 18 months. In some cases, OFAC simply never responds, effectively denying the application without taking formal action.

A denial by OFAC of a license application constitutes final agency action. The regulations do not provide for a formal process of appeal. However, OFAC will reconsider its determinations for good cause, for example, where the applicant can demonstrate changed circumstances or submit additional relevant information not previously made available to OFAC.

ACSS has provided detailed information on OFAC licensing in a webinar that is available at https://sanctionsalert.com/20170629past/.

Managing Licenses

It does an organization no good to have a license if the relevant personnel are not aware of it. If an organization does have licenses, it needs a system for personnel to identify and refer to the system. This could be something as simple as a spreadsheet showing the available specific licenses, with succinct descriptions of what they authorize. The system could also include relevant general licenses and exemptions.

Of course, the personnel should do more than just look at the description. Before proceeding with any transaction authorized by a license, a procedure should require the relevant personnel to review the license and ensure that it in fact authorizes the transaction. The procedure should include specific criteria to be reviewed, including the parties; the goods, services or technology involved; and the period for which the license is valid. The system should require documentation that the license was reviewed, and a short explanation of the grounds on which it was concluded that the license was applicable.

Other times an organization, especially a financial institution, may encounter a transaction requiring a license, where the license has been issued to another party. In the first place, the organization must have a policy as to whether it will engage in such transactions at all. It must also have a procedure detailing the requirements for reviewing the license and confirming that it authorizes, not just the party submitting the transaction, but the organization itself to proceed. If the organization is a bank, for example, and the transaction is submitted under a license to a customer, the bank must confirm that the license authorizes it as well as the customer to handle the transaction.

Blocking or Freezing

Sanctions laws of many jurisdictions, including the United States and the European Union, require that funds, assets, and other property be frozen (or, using the U.S. terminology, blocked). Frozen property cannot be transferred or disposed of without permission from the relevant government authority. In most cases, the party freezing the funds or other assets is required to report their action to the relevant authority.

In the United States, for example, a U.S. person blocking property must file a report with OFAC within 10 days.

Freezing is not the same thing as forfeiture. Title to the blocked property remains with the target. However, the exercise of powers and privileges normally associated with ownership is prohibited without authorization by the relevant authority. Blocking immediately imposes an across-the-board prohibition against transfers or dealings of any kind with regard to the property.

The first step in freezing is to determine that property must be frozen. A comprehensive screening system that identifies the sanctions applicable to a transaction or person, including a requirement to freeze assets, can help accomplish this. Further, the system must provide a procedure for “how” to freeze.

Typically, frozen funds or other property are placed in a designated and segregated account. Generally, funds must be placed in an interest-bearing account. Interest must be paid at a commercially reasonable rate. Some banks have opted to open separate accounts for each blocked transaction, while others have opted for omnibus accounts titled, for example, "Blocked Libyan Funds." Either method is satisfactory, so long as there is an audit trail which will allow specific funds to be unblocked with interest at any point in the future.

An institution may notify its customer that it has blocked funds in accordance with OFAC's instructions. The customer has the right to apply for the unblocking and release of the funds.

UNITED STATES DEPARTMENT OF THE TREASURY
OFFICE OF FOREIGN ASSETS CONTROL
REPORT OF BLOCKED TRANSACTIONS

INSTITUTION INFORMATION

INSTITUTION		TYPE OF INSTITUTION	ADDRESS
CITY	STATE	CONTACT PERSON	TELEPHONE NUMBER
POSTAL CODE	COUNTRY	E-MAIL ADDRESS	FAX NUMBER

TRANSACTION INFORMATION

AMOUNT BLOCKED	DATE OF TRANSACTION	DATE OF BLOCKING	PROGRAM OR REASON FOR BLOCKING FUNDS
ORIGINATOR NAME & ADDRESS		ORIGINATING FINANCIAL INSTITUTION NAME & ADDRESS	
INTERMEDIARY FINANCIAL INSTITUTION(S) NAME & ADDRESS		BENEFICIARY FINANCIAL INSTITUTION NAME & ADDRESS	
BENEFICIARY NAME & ADDRESS		ADDITIONAL RELEVANT INFORMATION (USE PAGE 2 IF MORE SPACE IS NEEDED)	
ADDITIONAL DATA FOUND IN ORIGINATOR TO BENEFICIARY INFORMATION OR BANK TO BANK INFORMATION			

PLEASE ATTACH A COPY OF PAYMENT INSTRUCTIONS AS PAGE 3 OF THIS FORM

PREPARER INFORMATION

SIGNATURE	NAME OF SIGNER	TITLE OF SIGNER	DATE PREPARED

OFAC Report of Blocked Transactions

The FFIEC BSA/AML Examinational Manual provides specific guidance in relation to blocked transactions.

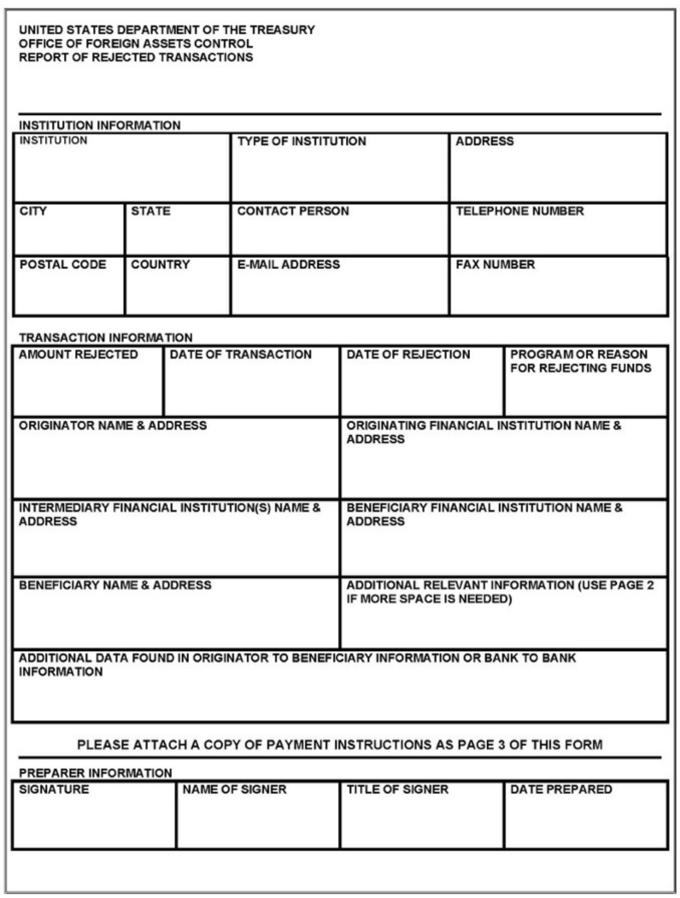
It states that U.S. law requires that assets and accounts of an OFAC-specified country, entity, or individual be blocked when such property is located in the United States, is held by U.S. individuals or entities, or comes into the possession or control of U.S. individuals or entities. For example, if 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.

Rejecting Transactions

Under some sanctions programs, especially in the United States, certain transactions are prohibited, but there is no requirement (or authorization) to freeze the funds involved. In such cases, a party must reject the transaction instead. It is vital that a party reviewing transactions correctly determine whether freezing or rejecting is required. In the United States, rejected transactions must be reported to OFAC within 10 days as well.



UNITED STATES DEPARTMENT OF THE TREASURY
OFFICE OF FOREIGN ASSETS CONTROL
REPORT OF REJECTED TRANSACTIONS

INSTITUTION INFORMATION

INSTITUTION		TYPE OF INSTITUTION	ADDRESS
CITY	STATE	CONTACT PERSON	TELEPHONE NUMBER
POSTAL CODE	COUNTRY	E-MAIL ADDRESS	FAX NUMBER

TRANSACTION INFORMATION

AMOUNT REJECTED	DATE OF TRANSACTION	DATE OF REJECTION	PROGRAM OR REASON FOR REJECTING FUNDS
ORIGINATOR NAME & ADDRESS		ORIGINATING FINANCIAL INSTITUTION NAME & ADDRESS	
INTERMEDIARY FINANCIAL INSTITUTION(S) NAME & ADDRESS		BENEFICIARY FINANCIAL INSTITUTION NAME & ADDRESS	
BENEFICIARY NAME & ADDRESS		ADDITIONAL RELEVANT INFORMATION (USE PAGE 2 IF MORE SPACE IS NEEDED)	
ADDITIONAL DATA FOUND IN ORIGINATOR TO BENEFICIARY INFORMATION OR BANK TO BANK INFORMATION			

PLEASE ATTACH A COPY OF PAYMENT INSTRUCTIONS AS PAGE 3 OF THIS FORM

PREPARER INFORMATION

SIGNATURE	NAME OF SIGNER	TITLE OF SIGNER	DATE PREPARED

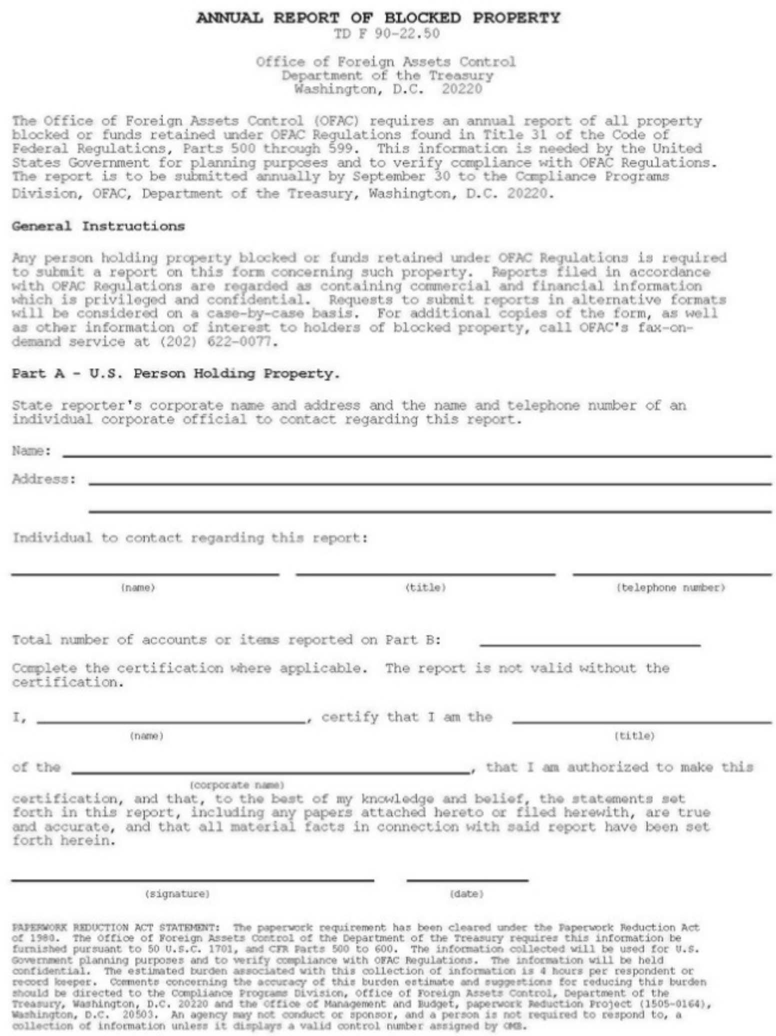
OFAC Report of Rejected Transactions

Record Keeping and Reporting

Record keeping and reporting are two important operational aspects of sanctions compliance. Record keeping requirements vary between countries. In the United States, OFAC requires that U.S. persons maintain records of transactions potentially subject to sanctions for at least five years:

Except as otherwise provided, every person engaging in any transaction subject to the provisions of this chapter shall keep a full and accurate record of each such transaction engaged in, **regardless** of whether such transaction is effected **pursuant to license or otherwise**, and such record shall be available for examination for **at least 5 years** after the date of such transaction. Except as otherwise provided, every person holding property blocked pursuant to the provisions of this chapter or funds transfers retained pursuant to §596.504(b) of this chapter shall keep a full and accurate record of such property, and such record shall be available for examination for the period of time that such property is blocked and for at least **least 5 years** after the date such property is unblocked.

The requirements to report to OFAC the freezing of property or rejection of transactions were discussed above. In addition, parties must file – by September 30 each year - an annual report regarding any property they have blocked.



ANNUAL REPORT OF BLOCKED PROPERTY
TD F 90-22.50

Office of Foreign Assets Control
Department of the Treasury
Washington, D.C. 20220

The Office of Foreign Assets Control (OFAC) requires an annual report of all property blocked or funds retained under OFAC Regulations found in Title 31 of the Code of Federal Regulations, Parts 500 through 599. This information is needed by the United States Government for planning purposes and to verify compliance with OFAC Regulations. The report is to be submitted annually by September 30 to the Compliance Programs Division, OFAC, Department of the Treasury, Washington, D.C. 20220.

General Instructions

Any person holding property blocked or funds retained under OFAC Regulations is required to submit a report on this form concerning such property. Reports filed in accordance with OFAC Regulations are regarded as containing commercial and financial information which is privileged and confidential. Requests to submit reports in alternative formats will be considered on a case-by-case basis. For additional copies of the form, as well as other information of interest to holders of blocked property, call OFAC's fax-on-demand service at (202) 622-0077.

Part A - U.S. Person Holding Property.

State reporter's corporate name and address and the name and telephone number of an individual corporate official to contact regarding this report.

Name: ______________________________

Address: ______________________________

____

Individual to contact regarding this report:

______________ (name) ______________ (title) ______________ (telephone number)

Total number of accounts or items reported on Part B: ______________

Complete the certification where applicable. The report is not valid without the certification.

I, ______________ (name), certify that I am the ______________ (title)

of the ______________ (corporate name), that I am authorized to make this certification, and that, to the best of my knowledge and belief, the statements set forth in this report, including any papers attached hereto or filed herewith, are true and accurate, and that all material facts in connection with said report have been set forth herein.

______________ (signature) ______________ (date)

PAPERWORK REDUCTION ACT STATEMENT: The paperwork requirement has been cleared under the Paperwork Reduction Act of 1980. The Office of Foreign Assets Control of the Department of the Treasury requires this information be furnished pursuant to 50 U.S.C. 1701, and CFR Parts 500 to 600. The information collected will be used for U.S. Government planning purposes and to verify compliance with OFAC Regulations. The information will be held confidential. The estimated burden associated with this collection of information is 4 hours per respondent or record keeper. Comments concerning the accuracy of this burden estimate and suggestions for reducing this burden should be directed to the Compliance Programs Division, Office of Foreign Assets Control, Department of the Treasury, Washington, D.C. 20220 and the Office of Management and Budget, paperwork Reduction Project (1505-0164), Washington, D.C. 20503. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number assigned by OMB.

OFAC Annual Report of Blocked Property

The initial report must contain the following information:

1. The name and address of the person holding the property blocked;
2. A description of any transaction associated with the blocking
3. The associated sanctions target(s) whose property is blocked (such as a Specially Designated National or other blocked person), the location(s) of the target(s) (if known), and, if not evident, a narrative description of the interest(s) of the target(s) in the property;

4. A description of the property that is the subject of the blocking and its location in the United States including any relevant account numbers and account types, check numbers, reference numbers, dates, or other information necessary to identify the property;
5. The date the property was blocked;
6. The actual or estimated value of the property in U.S. Dollars;.
7. The legal authority or authorities under which the property is blocked and any action taken with respect to the property; and
8. A copy of any payment or transfer instructions, check, letter of credit, accompanying bill of lading, invoice, or any other relevant documentation received in connection with any related transaction.

Reports on rejected transactions must include equivalent information.

Contractual Clauses and Warranties

While parties can conduct due diligence, they cannot foresee every eventuality with respect to sanctions compliance. One important method parties can utilize to reduce (though not eliminate) their sanctions risks is to use language in contracts to address sanctions issues. This typically takes the form of representations and warranties in contracts, such as loan agreements. Such representations and warranties typically include statements that:

- The party is not subject to sanctions by the UN, the EU, the United States, or other jurisdiction
- No person or entity owning more than a specified percentage of the company (usually either 10 percent or 25 percent) is subject to such sanctions
- The party is not currently under investigation by any authority for violations of sanctions laws
- In loan agreements, the party will not use the proceeds of the loan for investment in or transactions with parties or countries subject to sanctions by the UN, the EU, or the United States
- The party represents that performance of the contract on its part will not result in any violation of the enumerated sanctions laws

There is no standard form of such clauses, representations, or warranties. The following are examples of sanctions clauses that address these issues in a U.S. context, but which could easily be adapted to address sanctions regimes of other countries as well:

> The Company is not nor, to the knowledge of the Company, is any director, officer, agent, employee or affiliate of the Company currently subject to any U.S. sanctions administered by the Office of Foreign Assets Control of the U.S. Treasury Department ("OFAC"); and the Company will not directly or indirectly use the proceeds of the offering, or lend, contribute or otherwise make

> available such proceeds to any subsidiary, joint venture partner or other person or entity, for the purpose of financing the activities of any person currently subject to any U.S. sanctions administered by OFAC.
>
> Neither the Company nor, to the Company's knowledge, any director, officer, agent, employee or affiliate of the Company, is currently subject to any U.S. sanctions administered by the Office of Foreign Assets Control of the U.S. Treasury Department.
>
> The Borrower will not, directly or indirectly, use the proceeds of the Loan or lend, contribute, or otherwise make available such proceeds to any Subsidiary, other Affiliate of the Borrower, joint venture partner, or other Person to fund or facilitate any activities of or business or transaction with any Embargoed Person or any activities or business in any Sanctioned Country, or in any other manner that would result in a violation of any sanctions administered or enforced by OFAC, the U.S. Department of State, the United Nations Security Council, the European Union (EU), Her Majesty's Treasury, any EU member state, or other relevant sanctions authority (collectively, "Sanctions") by any Person (including, without limitation, any Person participating in the Loans, whether as underwriter, advisor, investor, or otherwise).

For trade finance transactions, the International Chamber of Commerce suggests standard language:

> Presentation of document(s) that are not in compliance with the applicable antiboycott, anti-money laundering, anti-terrorism, anti-drug trafficking and economic sanctions laws and regulations is not acceptable. Applicable laws vary depending on the transaction and may include United Nations, United States and/or local laws.

The ICC warns, however, against language that goes beyond compliance with laws to require compliance with company policies as well.

Interaction with Other Compliance Areas

Sanctions compliance is of course only one area within the general field of compliance. Sanctions compliance is closely associated with other areas of compliance, especially export controls and anti-money laundering. The following is a brief discussion of how these separate but related areas may interact.

Export Controls

Export controls and sanctions frequently intersect. Indeed, in some cases sanctions are administered under the export control laws. In the United States, for example, OFAC administers the sanctions regarding the export of services to Syria, while BIS is responsible for the regulation of exports of goods to Syria. In addition, export controls frequently apply to many of the same categories of goods as sanctions, especially arms. Organizations that import or export goods, services, or technology should have a separate system for complying with export control laws. In many situations, the sanctions and export control systems can share resources and expertise.

Anti-Money Laundering

Anti-money laundering (AML) also shares many similarities to sanctions compliance. The purpose of anti-money laundering controls is to prevent criminals from moving money from their criminal activities into the legitimate economy. Criminals use many of the same techniques to accomplish this that sanctions evaders employ, including shell companies, layering, and the use of cash.

Detecting and preventing money laundering also uses the same techniques as sanctions compliance. Chief among these are customer due diligence and transaction screening. The goal of customer due diligence is to identify the ultimate beneficial owners of assets to confirm that they are not criminals. Transaction screening in AML looks for patterns of suspicious transactions that indicate something other than legitimate business purposes. AML screening may also be useful in detecting sanctions evasion, precisely because the same techniques are used to "clean" dirty money and to evade sanctions. For this reason, it is important that the AML and sanctions compliance functions of banks in particular share information on an ongoing basis, as suspicious behavior detected by one function could be directly relevant to the other.

The following article from ACSS newsletter SanctionsAlert explains why compliance suits should treat sanctions as distinct from AML.

> *Seven Reasons Why Compliance Suites Should Treat Sanctions As Distinct from AML*
>
> *July 7, 2018*
> *By: SanctionsAlert.com*
>
> In recent times, the implementation of economic sanctions has been the go-to method for governments to put pressure on those countries that do not adhere to international standards. The implementation of economic sanctions as a leveraging tool has grown exponentially in the last decade and, as a result, given rise to a myriad of new rules and regulations that compliance suites must follow or suffer the consequences.

Nevertheless, despite this influx of new sanctions-based requirements, many compliance suites still continue to embed sanctions into their overall Anti-Money Laundering (AML)programs.

While it is true that sanctions and AML regimes have similar objectives and characteristics, such as the use of judgment; the importance of CDD/KYC; and the adoption of a risk-based approach, there are a number of significant differences between sanctions and AML that warrant treating them as distinct compliance genres.

1. Different Legal Basis

Reason #1	Sanctions	AML
Legal Basis	More numerous legal instruments, and country specific regimes	In the U.S., the main regulatory requirements are in the Bank Secrecy Act

Sanctions and AML regulations are based on differing legal bases.

In the U.S., AML regulatory requirements mostly derive from the Bank Secrecy Act (BSA) (1970), and its provisions. Additional legal requirements derive from, among others, the Money Laundering Control Act (1986), Annunzio-Wylie Anti-Money Laundering Act (1992), and the Money Laundering Suppression Act (1004).

The Bank Secrecy Act and its regulations are not "country-based".

As such, the suspicious activity reporting regime and AML program measures that a financial institution in the U.S. must taketo prevent and detect money laundering byan Italian organized crime group would be the same as those taken to prevent and detect money laundering by a Russian organized crime group.

This is different for sanctions. Because each program is based on different foreign policy and national security goals, prohibitions may vary between programs.

The core statutory basis for most of OFAC's country-based sanctions regimes is the International Emergency Economic Powers Act (IEEPA). This federal law, included in Title 50 (War and National Defense), Chapter 35, of the U.S. Code, provides continuing authority for the President—after a declaration of national emergency with respect to a particular threat—to regulate, in order to deal with that threat, among other things, transactions involving the property of foreign persons that is subject to U.S. jurisdiction.

Another important piece of legislation is the Trading With the Enemy Act, which was amended in 1941, grants to the president, during times of war or national emergency, the authority to prohibit or regulate trade, investments, remittances, travel, and virtually any economic transactions with any designated country or its nationals, wherever located.

The President exercises this authority simply by officially declaring what they believe to be a 'national emergency' and exercises this power by:

1. issuing **executive orders (EOs)**, which declare or reaffirm a previous declaration of national emergency, and which may block the property of certain entities, prohibit certain transactions;
2. order the heads of departments, in particular the Secretary of the Treasury, to issue **regulations** restricting certain activities.

The majority of country-based sanctions programs are **regulations** promulgated by the Secretary of the Treasury, pursuant to those executive orders, which enumerate prohibitions related to the country in question.

Examples of regulations issued under IEEPA:

31 CFR Part 510 – NORTH KOREA SANCTIONS REGULATIONS

31 CFR Part 535 – IRANIAN ASSETS CONTROL REGULATIONS

31 CFR Part 537 – BURMESE SANCTIONS REGULATIONS

31 CFR Part 538 – SUDANESE SANCTIONS REGULATIONS

31 CFR Part 541 – ZIMBABWE SANCTIONS REGULATIONS

31 CFR Part 542 – SYRIAN SANCTIONS REGULATIONS

31 CFR Part 543 – CÔTE D'IVOIRE SANCTIONS REGULATIONS

31 CFR Part 546 – DARFUR SANCTIONS REGULATIONS

31 CFR Part 547 – DEMOCRATIC REPUBLIC OF THE CONGO SANCTIONS REGULATIONS

31 CFR Part 548 – BELARUS SANCTIONS REGULATIONS

31 CFR Part 549 – LEBANON SANCTIONS REGULATIONS

31 CFR Part 551 – SOMALIA SANCTIONS REGULATIONS

31 CFR Part 560 – IRANIAN TRANSACTIONS AND SANCTIONS REGULATIONS

31 CFR Part 561 – IRANIAN FINANCIAL SANCTIONS REGULATIONS

31 CFR Part 562 – IRANIAN HUMAN RIGHTS ABUSES SANCTIONS REGULATIONS

31 CFR Part 570 – LIBYAN SANCTIONS REGULATIONS

31 CFR Part 576 – IRAQ STABILIZATION AND INSURGENCY SANCTIONS REGULATIONS

31 CFR Part 588 – WESTERN BALKANS STABILIZATION REGULATIONS

In contrast to AML, sanctions laws and regulations are different depending on the country, or group, that is targeted. Compliance suites will have to know these differences and make their decisions accordingly.

2. Fast-Changing Rules

Reason #2	Sanctions	AML
Fast-Changing Rules	Can be enacted by Congress, but often is quickly imposed by Presidential Executive Order	Laws enacted by Congress, regulations by FinCEN, only from time to time

In general, AML laws are less dynamic than sanctions laws.

Relatively speaking, AML requirements are only changed in a material way from time to time. One example is the USA PATRIOT Act of 2001, which changed the BSA in more than 50 instances and triggered many new BSA regulations. More recently, in 2016, FinCEN issued strengthened Customer Due Diligence (CDD) requirements for financial institutions. This regulation, however, became effective almost two years later, in May 2018, giving financial institutions ample time to prepare for the new requirements.

As Sanctions are usually enacted in response to a crisis or human rights violation, they are created in a much more volatile environment than their AML counterparts. Due to the frequent use of Executive Orders, which trigger new regulations issued by OFAC or other agencies, sanctions law and regulations often change much more quickly than AML law and regulations, giving rise to more complex compliance challenges, and less time for compliance departments to get prepare.

OFAC changes to sanctions regulations in June 2018

06/28/2018: Removal of the Sudan Regulations

06/28/2018: Publication of Global Magnitsky Regulations

06/27/2018: Revocation of JCPOA-Related General Licenses, Amendment of the Iranian Transactions and Sanctions Regulations

06/18/2018: Publication of Amended Rough Diamonds Control Regulations

06/04/2018: Issuance of Ukraine/Russia-related License

For example, last month alone, OFAC published the following changes in regulations on its website. These become effective after the date of publication in the Federal Register, which is typically in less than 30 days.

As such, sanctions requirements not only differ from AML requirements, but also require a compliance team to keep abreast of continual change in order to avoid getting into trouble with the regulator.

3. A Broader Scope

Not only are the legal instruments more numerous when it comes to sanctions, but their scope is more far reaching.

As is strictly defined by regulations, AML typically applies to "covered" entities, which includes financial institutions and other sectors particularly vulnerable to money laundering such as casinos and precious metal dealers. If the industry is not listed, the regulatory rules do not apply.

Reason #3	Sanctions	AML
Scope	Applies to all individuals and companies from all sectors	Typically applies to "covered" entities defined by AML regulations.

With sanctions, all U.S. persons must comply with the laws and regulations. This includes all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the U.S., all U.S. incorporated entities and their foreign branches. In the cases of certain

OFAC programs, 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.

This broad scope can create serious compliance challenges when dealing with sanctions, not only for limited industries, but individuals and all kinds of companies.

4. Fuzzy Guidance vs Prescriptive Rules

Sanctions guidance is also much harder to come by than advice on how to comply with BSA/AML rules.

For the most part, AML rules are prescriptive in nature. Often times, they will delineate exactly what is should be included in an AML program, going so far as to list the specific elements required, such as: Customer Identification Program (CIP), Customer Due Diligence (CDD), a designated AML officer, ongoing AML training, and periodic independent reviews.

Reason #4	Sanctions	AML
Guidance/Rules	Usually do not describe the process required to achieve compliance (exception: NYDFS Part 504)	Prescriptive – require an AML program with specific elements.

Sanctions compliance can be more challenging. With few exceptions, such as New York Department of Financial Services (NYDFS)'s Part 504 Rule, sanctions do not typically describe the process required to achieve compliance.

When it comes to sanctions, compliance teams must seek out alternative ways to make sure that their company is fully compliant.

5. Not the Same Focus and Targets

In addition to a broader scope, sanctions also focus on different behaviors and target alternate interests.

Typically, sanctions will focus on who (or where) you are whereas AML will focus on what you are doing. In other words, AML laws will target the proceeds of crime, while sanctions will target the property interests of sanctioned parties (i.e. through blocking of property/freezing of assets/prohibition of dealing with or provision of financial services to sanctions targets).

Example: Julio Suarez who lives in Venezuela owns a laundry front business that he uses to launder money, which he makes from his drug farm.

Reason #5	Sanctions	AML
Focus & Targets	Focuses on who (or where) you are and will target property interests of sanctioned parties	Focuses on what you are doing and the proceeds of crime from illicit activity

AML rules would focus on the money laundered through Julio's laundry business, and if Julio were your client and your company suspected unusual activity, you would have to file a Suspicious Transaction or Suspicious Activity Report (STR or SAR) with the relevant regulator.

Sanctions rules would target Julio himself, and/or his country, and potentially freeze his assets. For example, he personally may be included on OFAC's Specially Designated Nationals (SDN) List or fall under Venezuela's sanctions regime that targets certain industries. Your company would have to be aware of the specific sanctions regimes that would apply to Julio and then cease business with him. hough this can seem simple enough, fulfilling sanctions requirements can become complicated seeing as Julio Suarez may be a common name. Your business could have many customers with the name Julio Suarez and you may not be sure if your business' client is the same Julio Suarez who has been designated, or perhaps your team is uncertain whether or not Julio falls under Venezuela's targeted sanctions regime.

6. Real-Time vs. Post Facto Screening

In addition to different targets, sanctions and AML emphasize varying types of transaction monitoring.

Reason #6	Sanctions	AML
Screening/ Monitoring	Emphasize real-time screening	Generally post-facto monitoring of transactions

With the exception of client-onboarding and KYC, AML compliance generally consists of post-facto monitoring of suspicious transactions based on defined scenarios and complex behavioral typologies.

FinCEN, uses a threshold of $5,000 (or $2,000 for MSBs) for reporting suspicious transaction that could involve potential money laundering or terrorist financing.

On the flip-side, sanctions monitoring emphasizes real-time screening of transactions to make sure a client is not violating a sanctions regime or that a client has not been placed on a watch list, such as OFAC's SDN List.

Sanctions lists with designated persons and entities are constantly changing. Further, there is no minimum dollar threshold – any transaction is a violation. This makes the operationalization of real-time compliance a less than straight forward task.

7. Harsher Liability

Lastly, but certainly not least, sanctions have harsher compliance standards than AML. AML requirements incorporate risk-based compliance measures for violations and U.S. criminal laws typically require a wrongful (or wilful) state of mind as an element of any violation.

Reason #7	Sanctions	AML
Harsher Liability	Principle of strict liability	Typically based on willfulness

In contrast, OFAC sanctions rules employ a principle of strict liability. This means that a individual or company will be held accountable for violating sanctions even if there was no wrongful state of mind. OFAC emphasizes that individuals and entities will be held accountable regardless of the dollar value of the transaction at issue.

In other words, in our scenario above, if a financial institution processes a bank transfer for Julio Suarez involving drug proceeds, and there were no red flags of money laundering or no indicators of an unusual transaction, the government is likely to take this into account. However, if Julio was designated as an SDN, and the financial institution processed a transaction for him, without knowing he was designated, the financial institution can face OFAC penalties even if it didn't "know" about the violation.

The Business Environment and Sanctions

A final operational issue in sanctions compliance is the interaction between "the business" and the sanctions compliance function. Simply put, the business of the business is to make money. This is done by gaining customers and making sales.

Sanctions compliance, on the other hand, often requires an organization to forego business, however profitable it might be.

It is inevitable in such circumstances that there will be conflicts. The conflict may not be clear-cut. Personnel on the business side are commonly under enormous pressure to generate profits. In such circumstances, it is easy to take an aggressive approach towards sanctions while reassuring oneself that one is complying with the law. On the other side, sanctions compliance personnel may be told that all they ever do is to say "no," without necessarily understanding the complexities of or the pressures on the business side. Finally, there are cases, where even senior management simply decides that making money is more important than following the law.

Resolving these conflicts requires that both the business and compliance understand each other. It is vital that the sanctions compliance function understand the details of the organization's business, as well as the incentives the business side faces. It is equally vital that the business understand at least the broad outlines of the applicable sanctions laws, as well as the organization's sanctions policies and procedures. The ultimate goal is for the business side of the organization and the sanctions compliance function to work together in a manner that maximizes profits while minimizing exposure to sanctions risks.

Summary

- The sanctions compliance function needs clear procedures for resolving both standard and complex cases.
- Resolving complex cases may require going outside the compliance function for information and expertise.
- The effective use of licenses is a key part of any sanctions compliance system.
- This requires a system that identifies when licenses are necessary; prescribes the procedure for obtaining licenses; and ensures that the knowledge of available licenses is available throughout the organization.
- Organizations should have procedures for reviewing transactions to ensure that they are in fact covered by a license when necessary.
- An effective sanctions compliance system requires procedures detailing when and how to freeze or reject funds or assets.
- Record keeping and reporting are essential duties of any sanctions compliance system.
- Sanctions clauses, warranties, and representations can provide additional mitigation against sanctions risks.
- The sanctions compliance function must work closely with export controls and AML.
- The business and the compliance function must understand and communicate with each other.

Review Questions

1. What are the differences between general and specific licenses?
2. What should a license application include?
3. What are OFAC's requirements for reporting and record keeping?
4. Give three examples of sanctions clauses in contracts.
5. What are the similarities between AML and sanctions compliance?

ENFORCEMENT AND (INTERNAL) INVESTIGATIONS

Enforcement and Internal Investigations: Introduction

The sanctions laws impose obligations on those required to comply with them. Violating sanctions laws can trigger severe penalties, especially in the United States. The U.S. government has fined both U.S. and foreign companies billions of dollars for violations of U.S. laws. While other countries have not enforced their sanctions laws to the same extent, this could be changing.

The goal of a sanctions compliance system is to prevent sanctions violations. With even the best system, though, mistakes can occur. In such cases, it is important that the organization be able to investigate what happened and determine how to prevent it from happening again. It can then decide whether to disclose the possible violation to the relevant authorities, with the aim of reducing or even avoiding the legal penalties it might face.

The United States has by far the most thorough record regarding enforcement of sanctions laws. This chapter will therefore focus on U.S. law. However, many of the principles are applicable to sanctions compliance in other countries as well.

Enforcement Agencies

Sanctions laws may prohibit a national of a country, or even a foreign person, from doing some things, and require them to do others. U.S. law, for example, prohibits U.S. persons from doing business with SDNs, Crimea, Cuba, Iran, North Korea, or Syria, and prevent them from undertaking certain types of transactions involving Russia. U.S. requires U.S. persons to block property belonging to SDNs, to report certain types of transactions, and to maintain records. In some instances, these prohibitions apply to foreign persons as well, such as the prohibition on exporting services from the United States by clearing transactions through U.S. banks.

The United States has probably the most complex national systems of sanctions enforcement in the world. A number of different U.S. government agencies may be involved in the enforcement of the sanctions laws. These include OFAC, BIS, the Department of Justice, and the Federal Reserve. The New York Department of Financial Services has also played a major role in sanctions enforcement with respect to banks.

OFAC

The Office of Foreign Assets Control is an agency within the U.S. Department of Treasury. OFAC plays the primary role in administering and enforcing US sanctions programs. OFAC states that it

> administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation

of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States".

It is important to remember, though, that OFAC is not a regulatory agency. It does not provide oversight to any industry. Rather, OFAC is a national security agency whose primary mission is to protect the United States through enforcement of the sanctions laws. OFAC has an approximate $30-31 million budget and employs around 170 people, Mostly lawyers and intelligence analysts – reviewing classified intel reports, financial records, corporate registrations. Significantly, OFAC staff are recognized by Congress as essential personnel who are exempt from government shutdowns.

OFAC is responsible issuing the regulations implementing the sanctions laws. OFAC is responsible for enforcing those laws as well. OFAC has a wide investigative powers. However, because of its small size, it relies other regulators, especially of the financial industry, for assistance. These agencies include the Office of the Comptroller of the Currency and the Federal Reserve. OFAC also works closely with FinCEN, the U.S. financial intelligence unit, which is also within the Treasury Department and which enforces the anti-money laundering laws of the United States. OFAC also works closely with the Department of Commerce's Bureau of Industry and Security (BIS), which enforces the export control laws, and the State Department.

In May 2019, OFAC issued "A Framework for OFAC Compliance Commitments". This document is intended to provide organizations with a framework for the five essential components of a risk-based Sanctions Compliance Program (SCP), and contains an appendix outlining several of the root causes that have led to apparent violations of the sanctions programs that OFAC administers.

The document provides the following "root causes of OFAC sanctions compliance program breakdowns or deficiencies based on assessment of prior OFAC administrative actions":

1. Lack of formal OFAC SCP
2. Misinterpreting, or failing to understand the applicability of, OFAC's regulations
3. Facilitating transactions by non-US persons (including through or by overseas subsidiaries or affiliates)
4. Exporting or re-exporting US origin goods, technology or services to OFAC-sanctioned persons or countries
5. Utilizing the US financial system, or processing payments to or through US financial institutions, for commercial transactions involving OFAC sanctioned persons or countries
6. Sanctions screening software or filter faults

The document provides the following "root causes of OFAC sanctions compliance program breakdowns or deficiencies based on assessment of prior OFAC administrative actions":

1. Improper due diligence on customers/clients (e.g. ownership, business dealings, etc)
2. De-centralized compliance functions an inconsistent application of an SCP
3. Utilizing non-standard payment or commercial practices
4. Individual liability

See: https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf

FinCEN

Another US Treasury Department bureau that plays a significant if indirect role in sanctions enforcement is the Financial Crimes Enforcement Network, generally known as FinCEN. FinCEN collects and analyzes information, primarily from US financial institutions, about currency and electronic financial transactions and movements in order to combat domestic and international money laundering, terrorist financing, and other financial crimes. It also implements, administers and enforces compliance with the Currency and Foreign Transactions Reporting Act of 1970, commonly known as the Bank Secrecy Act, or BSA.

FinCEN enforcement actions do not deal with sanctions violations directly, but its investigation and enforcement of the anti-money laundering and terrorist financing laws may uncover sanctions violations as well. FinCEN can impose "Special Measures" under Section 311 of the USA Patriot Act (31 USC Section 5318A), which addresses sanctions violations, money laundering and terrorist financing. This provision authorizes FinCEN to impose "special measures" on financial institutions, nations or jurisdictions if it finds that they are of "primary money laundering concern." Special measures may prohibit or restrict the opening or operation of correspondent or payable-through accounts for a financial institution. FinCEN also issues guidance, especially for financial institutions, that is relevant to sanctions compliance as well as the preventing of money laundering.

BIS

The Bureau of Industry and Security (BIS) is the agency primarily responsible for enforcement of the export control laws of the United States. In particular, BIS issues licenses for the export of "dual-use" products, i.e., products that have both defense and civilian applications. BIS also regulates civilian items, called "EAR99" items. EAR99 items do not generally require a license for exportation from the United States, except to certain sanctioned countries, including Crimea, Cuba, Iran, North Korea, and Syria.

Like OFAC, BIS publishes lists, including the following:

- Denied Persons List: A list of individuals and entities that have been denied export privileges from the United States. Any dealings with a party on this list that would violate the terms of its denial order are prohibited.
- Entity List: A list of foreign parties that are prohibited from receiving some or all items subject to the EAR unless the exporter secures a license.
- Unverified List (UVL): A list of parties whose bona fides BIS has been unable to verify. No license exceptions may be used for exports, reexports, or transfers (in-country) to parties on this list. A statement must be obtained from such parties prior to shipping items not subject to a license requirement.

BIS does have certain direct sanctions duties. It rather than OFAC is responsible for licensing exports of goods (but not services) to Syria, and enforcing the U.S. ban on non-licensed or exempted exports to that country.

BIS investigates possible violations of U.S. export control laws and imposes penalties for violations. BIS works closely with OFAC, especially where an export control violation involves a country subject to sanctions. A leading example is the Huawei case, where BIS and OFAC cooperated in investigating a China company that was purchasing U.S.-origin products subject to export controls and then re-exporting them to Iran.

Department of State

The Department of State also direct responsibility for sanctions administration and enforcement in some areas. It is responsible for designating persons and entities who have violated U.S. secondary sanctions. The State Department may also designate as Foreign Terrorist Organizations (FTOs) foreign individuals or entities found to have committed, or which pose a significant risk of committing, acts of terrorism that threaten US national security, foreign policy, or its economy. Legally, the effect of designation as an FTO is similar to that for designation as an SDN. In conjunction with OFAC, State may also a range of entities, including terrorist groups, individuals who are part of a terrorist organization, and others such as financiers and front companies, as Specially Designated Global Terrorists (SDGTs). SDTGs are treated as SDNs. State may also designate individuals or entities for human rights abuses under the Global Magnitsky Act as SDNs.

The Directorate of Defense Trade Controls (DDTC), agency within the State Department, also administers the exportation of defense articles under the International Traffic in Arms Regulations (ITAR). ITAR applies specifically to defense articles, which include hardware and software technology, as well as services that may be used militarily, such as certain space-related items and technology. The ITAR contains the US Munitions List, which is a comprehensive list of all defense articles and services subject to ITAR and controlled by the DDTC.

The following article from ACSS newsletter SanctionsAlert explains the role of Department of State in designating terrorists.

The Relatively Little-Known Role of the U.S. State Department in Sanctioning Terrorists and its Consequences

December 5, 2017

In addition to the U.S. Treasury, the U.S. State Department has great influence over the implementation of U.S. sanctions policy in designating terrorists. Despite this important role, over 90% of compliance professionals recently polled by SanctionsAlert.com are either “not so familiar” with the State Department’s designations or “did not know” at all that it could designate.

The imposition of sanctions by the U.S. against terrorists, terrorist organizations, and their support structures is a powerful tool in the detection and prevention of terrorism.

At the State Department, this takes the form of two types of ‘designations’ on so-called “do not touch lists”, which it can use to deny individual terrorists and terrorist organizations access to the U.S. financial system; these include: Specially Designated Global Terrorists (SDGTs) and Foreign Terrorist Organizations (FTOs).

In a recent webinar at SanctionsAlert.com, Jason Blazakis, Director at the Office of Counter terrorism Finance and Designations at the U.S. Department of State – Bureau of Counter terrorism, discussed the role that the State Department plays in designating terrorists as well as the process employed by the State Department to make a terrorist designation.

The State Department’s Power to Designate

Mr. Blazakis launched his talk with an audience poll, which asked: “FTOs are designated by the Secretary of State in accordance with which law?” – The audience had a choice of three answers. Only 15% chose the correct answer.

In fact, the State Department’s power to apply FTO and SDGT designations to individuals and organizations derives from different sources. While the former derives from Section 219 of the Immigration and Nationality Act (INA), the latter derives from Executive Order 13224 pursuant to International Emergencies Economic Powers Act (IEEPA). In addition to their varying derivations, FTOs and SDGTs carry different consequences.

FTO Consequences:

- All funds under the control of a U.S. institution are frozen.
- Aliens are inadmissible to, and may be deportable from, the U.S.

- Illegal for persons subject to the jurisdiction of the U.S. to knowingly provide **material support** to the organization.
- Violators subject to civil and criminal penalties of up to 15 years imprisonment and fines.
- Provides the Department of Justice an **important prosecutorial tool**.

SDGT Consequences:

- Property and transactions under U.S. jurisdiction are frozen.
- Illegal to engage in transactions with designated individuals or entities.
- Criminal penalties of up to 10 years imprisonment and fines.
- Provides the Department of the Treasury the ability to make **derivative designations** of individuals and entities providing support to a designated individual or entity.

Most importantly, notes Blazakis, the FTO designation gives the Department of Justice (DOJ) a powerful tool to prosecute individuals, whether in the U.S. or abroad, who provide “material support”– a broad term contained in 18 U.S. Code 2339A, a 1996 federal terrorist law – to an FTO. According to Blazakis, “More than 50% of all counter terrorism prosecutions in the U.S. track back to some kind of link between an individual who is trying to provide material support and an FTO”.

The SDGT designation is more important to the U.S. Treasury Department as it allows them to make ‘derivative designations’ based on an individual’s SDGT status.Many times, the Treasury Department cannot make designations unless an individual/organization is first designated by the State Department.

Both FTOs and SDGTs are placed on OFAC’s “Specially Designated Nationals” (SDN) list. The SDN list is a compilation of persons and entities that are blocked or designated under a variety of sanctions programs. FTOs and SDGTs are identified on the SDN list with program code or tag “FTO” or “SDGT”.

The Step-by-Step Process of Making a State Designation

Mr. Blazakis goes on to identify the key steps in the process of making a designation by the State Department, which can take anywhere between 3-6 months to complete.

Firstly, the State Department must Identify a Target. Mr Blazakis explains that this involves identifying a potential individual or organization. In order to do this, the State Department will make their own determinations and also consider recommendations from other U.S. agencies, such as the Treasury Department. This usually takes only 1 week.

Once a target is identified, the State Department must conduct an Equity Check/Research. This involves drafting a few paragraphs outlining the individual or groups activities to identify if there are any sensitivities or overlap with other agencies. Often times, this is where a designation fails in furtherance of other, more important, overarching objectives. This step can take 1-3 weeks.

If the target survives the Equity Check, the State Department moves on to drafting an Administrative Record. Similarly drafted to a dissertation or thesis, the Administrative Record is a legal document that will form the fundamental background for the designation and is comprised of public information such as: news articles and Facebook posts, as well as classified information, such as: human intelligence reporting. This 'draft package' usually takes between 2-6 weeks to be put together.

Once the Administrative Record is created, the draft package is put through a highly bureaucratic Clearance Process. During this time, the Administrative Record must be reviewed by the DOJ and the Treasury, as well as their own legal team in order to make sure that the decision to move forward is backed up by solid evidence. This is the lengthiest part of the designation process and can sometimes take up to 3 months.

Once the Administrative Record is approved by all agencies, the package is sent to the Secretary of State for a Decision. It will be up to the Secretary of State whether or not to approve the designation. This step usually takes less than two weeks. If the designation is an FTO, Congressional Notification takes place. Congress is pre-notified 7 days before an individual or organization is formally designated. This notice is not required for SDGTs.

Lastly, the designation is published as a Federal Register Notice. At this point, the legal effects of the designation go into effect and the State Department will announce the designation through a press release.

The Process of Delisting

Often times, the delisting process is simply a reverse version of the designation process. There are, however, a few key differences between reversing an FTO as opposed to an SDGT.

When an FTO is challenged, it must be heard at the Federal Court of Appeal in the first instance, whereas a challenge to an SDGT can be brought at the District Level (i.e. one level lower). An FTO challenge must also be lodged within 30 days of the designation. After that time, it will be reviewed every 5 years, at which time the State Department will review whether the basis for designation has changed. If circumstances have in fact changed, it is mandatory for the State Department to delist the designation.

The Big Picture

The role of the State Department in sanctioning terrorists is not well known, but should not be overlooked. Just like U.S. Treasury's designations, U.S. State Department designations have broad consequences. "A terrorist designation doesn't just result in blocked assets and assets freeze. It does other things as well," says Mr Blazakis.

"An FTO designation provides the DOJ tools in the context of its prosecutions of individuals who may be engaged in "material support" and it provides leverage for DHS to declare individuals inadmissible to the U.S., if necessary," he explains.

Federal Reserve System

The Federal Reserve System is the central bank of the United States. While the Federal Reserve's primary responsibilities are to maintain monetary stability and promote employment, it has some bank supervisory and regulatory functions. These include supervision over the foreign activities of U.S. banks and the U.S. activities of foreign banks. The Federal Reserve is also responsible for supervision of bank holding companies. The Federal Reserve will investigate whether banks subject to its supervision have committed sanctions violations, although its focus is primarily on any deficiencies in banks' sanctions compliance system. Along with OFAC, the Federal Reserve has been involved in a number of cases involving violation of U.S. sanctions laws by foreign banks.

Department of Justice

The Department of Justice (DOJ) is the law enforcement agency of the U.S. federal government. Although Justice does not administer the sanctions laws, it may be involved if a sanctions violation rises to the level of a criminal case. In particular, Justice will become involved if OFAC, BIS, FinCEN, or some other federal agency makes a criminal referral to it for willful violations of the sanctions, export control, or anti-money laundering laws.

Under the International Emergency Economic Powers Act (IEEPA), it is a crime to willfully violate, or attempt to violate, any regulation issued under the act. Because most sanctions regulations (except for those involving Cuba) are issued under IEEPA, this encompasses most U.S. sanctions. Typically, OFAC will begin a sanctions investigation. If the investigation uncovers what appear to be willful violations of sanctions laws, OFAC may make a criminal referral to DOJ. At that point, DOJ will join in the investigation. If there is an actual prosecution, DOJ will handle that as well. As a practical matter, though, most such investigations are settled. DOJ has obtained settlements involving violations of U.S. sanctions and export control laws totaling billions of U.S. dollars.

In October 2016, the Department of Justice, National Security Division issued "Guidance Regarding Voluntary Self-Disclosures, Cooperation, and Remediation in Export Control and Sanctions Investigations Involving Business Organizations". The Guidance memorializes the policy of NSD to encourage business organizations to voluntarily self-disclose criminal violations of the statutes implementing the U.S. government's primary export control and sanctions regimes – the Arms Export Control Act (AECA), 22 U.S.C. § 2778, and the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1705.2 The Guidance applies only to export control and sanctions violations. Because financial institutions often have unique reporting obligations under their applicable statutory and regulatory regimes, the Guidance does *not* apply to financial institutions.

The Guidance aims to provide greater transparency about what is required from companies seeking credit for voluntarily self-disclosing potential criminal conduct, fully cooperating with an investigation, and remediating. Accordingly, the Guidance

1. first explains what constitutes a VSD, full cooperation, and timely and appropriate remediation.
2. Second, the Guidance provides examples of aggravating factors that, if present to a substantial degree, could limit the credit an organization might otherwise receive, though the company would still find itself in a better position than if it had not submitted a VSD, cooperated, and remediated.
3. Third, the Guidance explains the possible credit that may be afforded to a business organization that complies with the mandates set out below, including the disclosure of all relevant facts about the individuals involved in the wrongdoing.
4. Finally, the Guidance provides sample scenarios that demonstrate the application of this policy.

The Guidance sets forth that, ordinarily, when an organization voluntarily self-discloses violations of U.S. export controls and sanctions, it presents its VSD to the appropriate regulatory agency under the procedures set forth in the agency's regulations. It is not the purpose of this Guidance to alter that practice.

Business entities should continue to submit VSDs to the Department of State, Directorate of Defense Trade Controls (DDTC) for violations of the International Traffic in Arms Regulations (ITAR); to the Department of Commerce, Bureau of Industry Security (BIS) for violations of the Export Administration Regulations (EAR); and to the Department of the Treasury, Office of Foreign Assets Control (OFAC), for violations of U.S. sanctions regulations. When an organization becomes aware that the violations may have been willful, it should within a reasonably prompt time *also* submit a VSD to NSD's CES (Counterintelligence and Export Control Section).

New York Department of Financial Services

The New York Department of Financial Services (DFS) is the agency of the State of New York responsible for regulating financial institutions in New York. Practically all large U.S. banks and international banks doing business in the United States have branches in New York. As a practical matter, most international transactions denominated in U.S. dollars are cleared through banks in New York. This gives DFS wide oversight powers over international banking transactions in particular.

New York law makes it a violation for a bank to

- Conduct business in an unsafe and unsound manner
- Fail to maintain an effective sanctions compliance program
- Knowingly make false entries in its books and records
- Omit material from its books and records with the intent to mislead
- Fail to make available books and records of all transactions and actions
- Fail to submit a report to the appropriate authorities upon the discovery of fraud, dishonesty, false entries, or omission of entries

DFS has used these laws as the basis for fines totaling billions of dollars against foreign banks for violations of U.S. sanctions laws committed in connection with transactions that occurred in New York, and in particular the clearing of U.S. dollar transactions through New York. In these cases, DFS has worked closely with OFAC and DOJ.

The Investigative Process

One of two events may trigger an investigation by OFAC. First, OFAC may receive information indicating a sanctions violation. This could come from a whistleblower inside an organization or from an outside party, such as a bank, supplier, or customer. Alternatively, an organization may file a self-disclosure with OFAC, describing a potential violation of the sanctions laws.

In either case, OFAC will launch an investigation. There is typically no public notice that an investigation has begun, and OFAC has no requirement to inform the target of the investigation, known in OFAC terminology as the Subject Person. However, at some point OFAC will usually contact the Subject Person, inform them of the investigation, and request information. Of course, in cases of self-disclosure, the Subject Person is aware that OFAC may be investigating it.

Possible OFAC Actions

As described below, OFAC can conclude an investigation in a number of ways, including settlement.:

1. No action. OFAC concludes that no violation occurred, that the information it has is insufficient to establish a violation, or that there was a violation, but it does not rise to the level of warranting an administrative response. The Subject Person may be informed of this decision, especially if it was aware of the investigation. Although OFAC does not publish statistics on it, this is probably the most common outcome of OFAC investigations.
2. Cautionary letter. OFAC will issue a cautionary letter if it finds that the evidence does not support a finding of a violation, or that a violation does not warrant a finding of violation or monetary penalty, but that the conduct identified could lead to violations in the future.
3. Finding of a violation. This is a formal decision by OFAC that a violation has occurred, considers it important to document the occurrence of a violation and concludes that the Subject Person's conduct warrants an administrative response but that a civil monetary penalty is not appropriate.
4. Civil monetary penalty. OFAC imposes a monetary penalty on the Subject Person. The amount of the penalty will be based on the factors discussed below.
5. Criminal referral. If the conduct identified by the OFAC investigation indicates criminal conduct, OFAC may refer the matter to other law enforcement agencies for further investigation and action. The most common recipient of criminal referrals by OFAC is DOJ.
6. Other administrative action. In appropriate circumstances, OFAC may impose other administrative penalties, including
7. Denial, modification, suspension, or revocation of licenses
8. A cease and desist order directing the Subject Person to cease prohibited conduct.

Settlement

OFAC and the Subject Person may also settle an investigation. In a settlement, OFAC and the Subject Person agree on any penalties and action required. Either party can initiate settlement discussions. Settlement is of course totally at the discretion of OFAC. As a practical matter, settlement is probably the most common outcome in investigations where OFAC has decided to impose a monetary penalty. Besides paying a civil penalty, a settlement agreement may also require the Subject Person to undertake certain actions. A common requirement is that the Subject Person demonstrate after a fixed period that its sanctions compliance system can effectively detect and prevent sanctions violations. A settlement is not considered final agency action for legal purposes, so that the matter can be reopened by either party. In fact, settlement agreements generally give OFAC the authority to reopen the investigation if the Subject Person does not comply with the terms of the settlement.

The Penalty Notice Procedure

In cases where it determines to impose a civil monetary penalty, OFAC follows a formal procedure. These steps are:

1. The initial investigation
2. Pre-penalty notice: a formal notice to the Subject Person that OFAC has preliminarily determined that a violation has occurred. The notice will include a description of the violation and the proposed penalty.
3. Response to the pre-penalty notice. The Subject Person has an opportunity to respond to the pre-penalty notice. It can agree with the notice, or argue that either there was no violation, or that the penalty should be less than that proposed by OFAC.
4. Penalty notice. This is OFAC's formal notice that it is imposing a civil penalty. It constitutes final agency action for legal purposes.
5. Referral to the Financial Management Division. The issuance of a penalty notice creates a debt the Subject Person owes the U.S. federal government. The Financial Management Division is the actual collector of the debt.

Penalties

The penalties for violating sanctions laws can be severe. Most penalties for sanctions violations take the form of civil penalties imposed by OFAC. OFAC will consider a number of factors in deciding whether to impose a penalty, as well as the nature and amount of the penalty.

Base Amounts for Penalties

Most sanctions programs are controlled by IEEPA. Under IEEPA, the maximum penalties for sanctions violations include:

- Civil penalties in the amount of the greater of $250,000 or twice the value of the transaction. In fact, the maximum fine is periodically adjusted for inflation; the current maximum is $289,238, unless this amount is less than twice the value of the transaction.
- A criminal fine of up to $1,000,000
- If a natural person committed the violation, imprisonment for up to 20 years
- Any violation of IEEPA, or any orders or regulations promulgated under it, can lead to a penalty. The violation does not have to be willful to result in a penalty. Criminal penalties, however, do require prove that the violation was willful.

The OFAC Factors

OFAC can only impose civil penalties. OFAC's procedure for imposing penalties, and the factors it takes into account, are set forth in OFAC's Economic Sanctions Enforcement Guidelines, which are included in the reference materials. In determining the amount of the penalty, OFAC will consider a number of factors, including:

1. Willfulness: the conduct at issue was willful. OFAC will consider whether
   a. The Subject Person knew their conduct violated the law.
   b. The Subject Person acted in reckless disregard for
   c. The violation reflects a pattern of conduct on the part of the Subject Person.
   d. The Subject Person had prior notice that its conduct might violate the law.
   e. Management was involved in the conduct.
2. Awareness: the extent to which the Subject Person was aware of the conduct giving rise to a violation. Evidence of awareness is present if
   a. The Subject Person had actual knowledge of the conduct.
   b. The Subject Person should have known about the conduct.
   c. Management was involved in the conduct.
3. Harm to sanctions objectives: the effect of the violation on the ability of the United States to achieve the goals of the sanctions in question. Factors OFAC will consider include
   a. The economic benefit of the violation to the sanctioned individual, entity, or country
   b. The implications for U.S. policy
   c. Whether a license was available for the conduct in question
   d. Whether the conduct was in support of humanitarian activity
4. Individual characteristics: the various characteristics of the Subject Person that OFAC considers relevant, including
   a. Size
   b. Sophistication
   c. Volume of transactions

d. Volume of transactions
e. Past sanctions history
f. Existence, nature, and adequacy of a sanctions compliance program
g. The organization's remedial response upon learning of the conduct

5. Cooperation with OFAC: once the investigation started, whether the Subject Person responded adequately to OFAC's requests for information
6. Timing: whether the violation occurred shortly after a change in the applicable sanctions
7. Future compliance and deterrence effects: to what extent OFAC action might deter others from engaging in similar conduct in the future, and instead encourage compliance

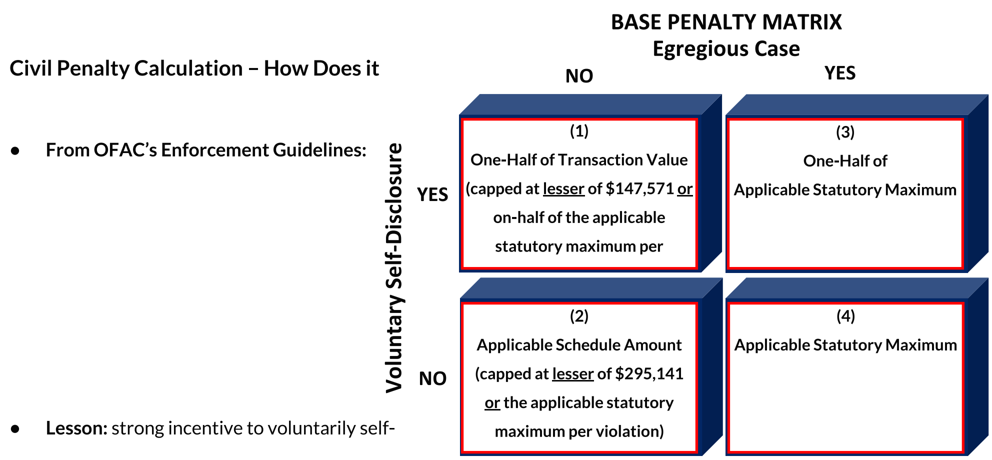
OFAC will consider all of these factors in deciding what action to take. If it decides to impose a penalty (or agree to a negotiated penalty), OFAC will consider in particular whether the conduct was "egregious," and whether the Subject Person performed a self-disclosure. In assessing egregiousness, OFAC looks at Factors 1-4 above:

- Willfulness
- Awareness
- Harm to sanctions objectives
- Individual characteristics

Applying these factors, the guidelines indicate that OFAC may reduced penalties by up to 50 percent of the base penalty, which is the statutory maximum under IEEPA.

For purposes of OFAC civil penalties, the value of a transaction means the dollar value of the goods or services involved in subject transaction. Significantly, for financial transactions, the value of the transaction is the nominal amount involved. Thus, if a bank illegally processes a payment worth $1 million, the value of the transaction would be $1 million, rather than the bank's processing fee. For this reason, the transaction values in violations involving banks in particular can be very large.

OFAC Enforcement



Source: ACSS OFAC Essentials Online Certificate Course

The following article on sanctionsassociation.org provides tips how to comply with an OFAC settlement.

Ten Tips On How To Comply With An OFAC Settlement Agreement (Or Avoid the Regulator Altogether)

April 23, 2019
By Scott Nance, Principal Langley Compliance

Recent times have seen an uptick in sanctions enforcement actions, placing an onus on many compliance suites and officers to take head and build a robust sanctions compliance program.

In April 2019 alone, OFAC concluded settlement agreements with Standard Chartered Bank, three UniCredit Bank companies, an oilfield services provider, and Stanley Black & Decker (a well-known U.S. tool manufacturer). As all agreements follow a very similar pattern, it is safe to assume that OFAC has decided upon a standard set of requirements for all companies to be compliant. Whether you are a company who has been recently fined by OFAC or are looking to avoid being fined by the regulator, these top tips should assist you in trying to stay ahead of the game.

Standard OFAC Requirements

In addition to paying a fine, recent settlement agreements all impose certain commitments with respect to an entity's sanctions compliance program.

These commitments include:

- A commitment by management to sanctions compliance;
- An assessment of sanctions risk;
- Implementation of an adequate system of internal controls;
- Periodic testing and audits of the sanctions compliance system;
- Sanctions training; and
- An annual certification for five years that the system satisfies these requirements. This settlement agreement model requires the first certification to be no more than 180 days after the agreement is signed. This means a company only has six months to fulfill all the above requirements and bring their program up to scratch. Such a short deadline places a premium on prior planning.

Ten Tips on Fulfilling OFAC Settlement Requirements

When working as ING's Head of Global Sanctions Compliance from 2013to 2014, one of my chief responsibilities was to help ensure that ING satisfied the terms of its settlement agreement with the United States. During that process, I learned a number of lessons that may provide some assistance to companies – whether they are banks, manufacturers, or service providers – that find themselves dealing with an OFAC settlement agreement. Much of this can also be applied to those seeking to avoid attention from the regulator.

1. Assemble a team responsible for the process. It is essential to form a team at the very beginning that will have primary responsibility for doing whatever must be done to comply/stay compliant. Though the team will normally consist of experienced personnel from Compliance and Legal, it may also include representatives from the business side of the company, as well as personnel from more technical areas, such as trade finance or export processing. If your organization is not a U.S. company, be sure to involve at least one expert on U.S. sanctions as well. While it is fine to call upon at least some external assistance to provide specialized expertise, do not be tempted to outsource the entire process. OFAC compliance requires a thorough understanding of the bank's internal policies and procedures. In addition, because the system will continue to operate after any outside experts are gone, your own personnel should take the lead.
2. Assign one or two people to take primary responsibility for the process. Managing the compliance process will not necessarily be a full-time job, but it may be close to it. You need someone to oversee the process to ensure that progress is being made on a day-to-day basis.
3. Identify exactly what the settlement agreement requires, and assign responsibilities for each obligation. A settlement agreement typically imposes a number of requirements. Some of them may be very specific, while others are extremely broad. An obvious starting point is to go through the agreement in detail and assign someone on the team explicit responsibility and authority to address each requirement. If

you are looking to enhance your compliance system, use the OFAC commitments as your guidelines.

4. Decide who is / how you are going to certify. The new standard settlement agreement simply says that a "a senior-level executive or manager" must make the annual certification. An important first step is to decide who will conduct the actual review of compliance with the terms, and who this certifying executive will be. As important is to specify the process for certification. The responsible executive cannot simply decide at the end "yes, we're good." You need to specify how the process will work, including when and in what form the responsible executive will receive the necessary information. A schedule should be an intrinsic part of the process, to make sure that you're not trying to do everything at the last minute.

5. Agree on the terms of certification. Although they now provide more detail, the new model of OFAC settlement agreements still leaves many questions open about certification requirements. For example, the recent OFAC agreements require that a company's compliance system include "written policies and procedures outlining its sanctions compliance program." They do not say what policies and procedures an adequate sanctions compliance program should include. The team should identify at the start the components of such a program, so that there is a clear guide for certification. The same is true with respect to the other terms, including management commitment, risk assessment, review and audit, and training.

6. Draw upon internal technical expertise, when necessary. In the course of reviewing your company's compliance system, it is likely that highly technical issues will arise in connection with policies and procedures over such topics as payments or trade finance. The team should be able to identify and draw upon the company's internal experts to resolve these issues.

7. Provide adequate training to the certifiers. To ensure objectivity, some function other than Compliance or Legal is likely to make the certification. Internal Audit is an obvious choice. However, it is likely that the people conducting the review know little if anything about sanctions. It is essential to provide them with training at the very start of the process so that they understand exactly what it is they're do in

8. Set up rules of governance. There will be disagreements during the certification process. Your organization should establish rules of governance at the very beginning to specify who is authorized to make decisions, and how the inevitable disagreements will be resolved. Ultimately, this may require a decision by top management or the Supervisory Board/Board of Directors. If you set up the rules of governance at the beginning, you can avoid time-consuming arguments later.

9. Use this as an opportunity to improve your compliance system. As a result of the compliance process, you will end up examining its sanctions compliance system in great detail. This provides an excellent opportunity not just to identify gaps in the system, but also to assess how the system is working and how it can be improved.

10. Be patient. The process of complying with a settlement agreement can be frustrating. Try and be as patient as possible. If you're organized, have set up a team and a manager, fixed a schedule, and agreed on exact certification requirements, then the process will most likely be a success. Moreover, you will find your sanctions compliance system is stronger and more effective than ever before.

Internal Investigations and Voluntary Self-Disclosure

Organizations frequently discover potential sanctions violations on their own. In such cases, the organization should start with an internal investigation. It can then decide whether to perform a voluntary self-disclosure to the appropriate government agency.

Internal Investigations

Someone in an organization sees information that indicates to them that a sanctions violation might have occurred. The appropriate response is to conduct an internal investigation. The investigation may be very brief; the person may have misunderstood the applicable law, for example. Other times, investigations can be very long and complex, taking years and costing millions of dollars. The steps in conducting an internal investigation, though, are generally the same. The following summary is excerpted from Performing a Look-Back Review of Transactions for Potential Compliance Violations, an article written by Scott Nance, an attorney specializing in sanctions.

Step 1: Understand exactly *why* there might be a problem. To achieve this understanding, the organization needs answers to key questions:

1. What were the transactions involved?
2. What laws or regulations might have been violated?
3. How was the problem discovered, by who, and when?
4. What is the applicable law?

Answering these questions will probably require gathering information, and may well require the cooperation of various divisions or departments. It may be necessary to consult the organization's legal function, and even to consult outside experts. The aim of Step 1 is to determine the basic facts and whether additional investigation is necessary.

Step 2: Determine who in management must be informed. This will depend to a large extent on the institution's internal organization, as well as on the specifics of the situation. At a minimum, the head of compliance, as well as the legal department, should probably be informed. If the initial review confirms that there may be a problem, it may be a good idea to consult outside counsel at this point as well.

Step 3: Assess the organization's overall compliance situation. To understand how the violation might have occurred, it is necessary to understand exactly how the institution manages compliance in these situations. This will also allow the organization to identify what relevant data might be available. An obvious starting point are the organization's sanctions procedures and policies, and in particular how individual transactions are examined for possible sanctions export control issues.

Step 4: Determine whether and to what extent a look-back of transactions is necessary or advisable. A look-back is an investigation of past transactions as well as the transaction or situation that triggered the process. This is necessary to determine whether the problem might have happened in the past, but not been identified. The main steps in performing a look-back are:

1. Define the universe of transactions or records that need to be examined.
2. Identify, as specifically as possible, what information a search of these transactions should provide.
3. Perform the search itself to collect the relevant information.
4. Review the information and identify whether it indicates that additional violations may have occurred in the past.

Step 5: Decide what to do next.

1. If the investigation reveals possible violations, consider whether and how to disclose this to the authorities.
2. Even if the internal investigation does not reveal any potential sanctions violations, it may have identified deficiencies in the compliance system. This is an opportunity to correct those deficiencies before they cause actual legal problems.

Voluntary Self-Disclosure

Self-disclosure of potential sanctions violations in the United States is not mandatory; that is why it is called "voluntary." Self-disclosure, though, is a mitigating factor, and can lead OFAC to reduce penalties significantly.

The OFAC enforcement guidelines define "self-disclosure" as

> Self-initiated notification to OFAC of an apparent violation by a Subject Person that has committed, or otherwise participated in, an apparent violation of a statute, Executive order, or regulation administered or enforced by OFAC, prior to or at the same time that OFAC, or any other federal, state, or local government agency

> or official, discovers the apparent violation or another substantially similar apparent violation. …

To obtain full credit for the disclosure, OFAC states that

> A voluntary self-disclosure must include, or be followed within a reasonable period of time by, a report of sufficient detail to afford a complete understanding of an apparent violation's circumstances, and should also be followed by responsiveness to any follow-up inquiries by OFAC.

A voluntary disclosure the first, and probably best, opportunity to describe the facts and frame the issues in a manner that most accurately reflects the organization's behavior. The voluntary disclosure should begin with a brief description of the problem (such as failure to report cash transactions or the processing of transactions that violated export control laws). The disclosure should describe how the institution initially discovered that there might be a problem, and the steps it took to investigate. The disclosure should of course describe the results of the investigation, and the factual and legal conclusions upon which the organization reached the conclusion that a potential sanctions violation may have occurred.

A voluntary disclosure is not simply a factual submission. It gives the Subject Person the opportunity to present its case in the best possible light while providing complete and accurate information. It also gives the organization the opportunity to explain how it is addressing the problem. OFAC and other enforcement agencies, including DOJ, will consider attempts to mitigate the situation, and to prevent it from arising again, in deciding what action to take. For this reason, the voluntary disclosure should include a description of what the organization has done to prevent the situation from recurring, such as the institution of new procedures.

For non financial institutions, please also refer to the DOJ Guidance on VSD discussed earlier in this chapter.

Summary

- A number of different agencies in the U.S. government, including OFAC, BIS, the State Department, and the Federal Reserve, share responsibility for enforcing the sanctions laws.
- The Department of Justice undertakes criminal prosecutions for sanctions laws.
- The New York Department of Financial Services may apply New York law to sanctions violations that occurred in New York.
- OFAC may conclude a sanctions investigation by
    - Taking no action
    - Issuing a cautionary letter

    - Publishing a finding of violation
    - Imposing a civil monetary penalty
    - Making a criminal referral
- In deciding whether to impose penalties, as well as the type and scale of penalties to impose, OFAC will consider a number of factors.
- Self-disclosure to and cooperation with OFAC can reduce penalties significantly.
- A self-disclosure gives an organization the opportunity to present its case to OFAC, and can result in reductions of penalties.

Review Questions

1. What are the sanctions responsibilities of the U.S. State Department?
2. What is the determining factor in criminal penalties under IEEPA?
3. Name five factors OFAC considers in assessing penalties.
4. Give the steps in an internal investigation.
5. What are the benefits of voluntary self-disclosure?

REFERENCE MATERIAL AND READING LIST

Association of Certified Sanctions Specialists (ACSS)
7950 NW 53rd Street Suite 337
Miami, FL 33166
Phone: +1 305 433 7187
helpdesk@sanctionsassociation.org
www.sanctionsassociation.org

Association of Certified Sanctions Specialists (ACSS)

www.sanctionsassociation.org

Bureau of Industry and Security - BIS

https://www.bis.doc.gov/

COMMISSION RECOMMENDATION (EU) 2019/1318 of 30 July 2019 on internal compliance programmes for dual-use trade controls under Council Regulation (EC) No 428/2009

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN

Department of Justice - Criminal Division - Evaluation of Corporate Compliance Programs Guidance Document (April 2019)

https://www.justice.gov/criminal-fraud/page/file/937501/download

European Union - Basic Principles on the Use of Restrictive Measures

http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010198%202004%20REV%201

European Union - Restrictive Measures (Sanctions) - Update of the EU Best Practices for the Effective Implementation of Restrictive Measures

http://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/en/pdf

European Union - Sanctions Guidelines - Update (May 4 2018)

https://data.consilium.europa.eu/doc/document/ST-5664-2018-INIT/en/pdf

European Union - Commission

https://ec.europa.eu/fpi/what-we-do/sanctions_en

European Union – Council of the European Union

https://www.consilium.europa.eu/en/policies/sanctions/

E.O. 13871 of May 8, 2019 Imposing Sanctions in Respect to the Iran, Aluminium, and Copper Sectors of Iran

https://www.treasury.gov/resource-center/sanctions/Programs/Documents/13871.pdf

FFIEC BSA/AML Examination Manual - CORE EXAMINATION PROCEDURES FOR REGULATORY REQUIREMENTS AND RELATED TOPICS - Office of Foreign Assets Control—Overview

https://bsaaml.ffiec.gov/manual/RegulatoryRequirements/15

Financial Action Task Force Recommendations

http://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate)

Financial Action Task Force - Financing of Proliferation

http://www.fatf-gafi.org/publications/financingofproliferation/?hf=10&b=0&s=desc(fatf_releasedate)

Financial Action Task Force – International Best Practices – Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6)

http://www.fatf-gafi.org/media/fatf/documents/recommendations/BPP-Fin-Sanctions-TF-R6.pdf

Government of Canada - Sanctions

https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/index.aspx?lang=eng

New York Department of Financial Services (NYDFS) - Part 504 Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications

https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsp504t.pdf

OFAC Main Website

https://www.treasury.gov/about/organizational-structure/offices/Pages/office-of-Foreign-Assets-Control.aspx

OFAC Framework for OFAC Compliance Commitments

https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf

OFAC 50% Guidance

https://www.treasury.gov/resource-center/sanctions/Documents/licensing_guidance.pdf

OFAC FAQ

https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_general.aspx

OFAC Enforcement Actions

https://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx

OFAC licenses

https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_general.aspx#licenses

OFAC North Korea Sanctions and Enforcement Advisory - Risks For Businesses with Supply Chain Links to North Korea

https://www.treasury.gov/resource-center/sanctions/Programs/Documents/dprk_supplychain_advisory_07232018.pdf

OFAC North Korea Sanctions Advisory "Sanctions Risks Related to North Korea's Shipping Practices"

https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/dprk_vessel_advisory_02232018.pdf

OFAC's Economic Sanctions Enforcement Guidelines

https://www.treasury.gov/resource-center/sanctions/Documents/fr74_57593.pdf

Office of Financial Sanctions Implementation - OFSI (UK)

https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation

Wolfsberg Group Guidance on Sanctions Screening

https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf

United Nations

https://www.un.org/securitycouncil/sanctions/information

31 CFR 560.208 – Prohibited facilitation by United States persons of transactions by foreign persons

https://www.law.cornell.edu/cfr/text/31/560.208

GLOSSARY OF SANCTIONS TERMS

Association of Certified Sanctions Specialists (ACSS)
7950 NW 53rd Street Suite 337
Miami, FL 33166
Phone: +1 305 433 7187
helpdesk@sanctionsassociation.org
www.sanctionsassociation.org

A

ABA Export Controls & Economic Sanctions Committee: This American Bar Association committee follows US, Canadian and other export controls and embargoes and sanctions programs.

AFMLS: Asset Forfeiture and Money Laundering Section of the US Department of Justice. AFMLS pursues prosecutions against institutions and individuals engaged in money laundering, Bank Secrecy Act violations and sanctions violations.

AIS: Automatic Information System transponder that automatically and continually reports the position of a ship.

aka: Acronym for "also known as," commonly used on sanctioned entities or persons lists in reference to an alias or multiple aliases or multiple spellings of an individual's name. Sanctions lists such as the OFAC SDN list contain many AKAs. OFAC includes these AKAs because, based on information available to it, the sanctions targets refer to themselves, or are referred to, by these names. See also weak AKA.

Alert spike: A substantial increase in the number of alerts generated. A spike could be caused by, for example, remediation exercises, changes or updates to policies, procedures or watchlists. This definition is provided in the Wolfsberg Screening Guidance.

Al-Qaida Sanctions Committee's "Assets Freeze: Explanation of Terms": Document approved by the UN Security Council ISIL (Da'esh) & Al-Qaida Sanctions Committee on February 24, 2015. Sets forth objectives of the assets freeze as set out in paragraph 1 (a) of resolution 2161 , the scope of assets freeze, plus exemptions and definitions related to assets freeze.

AML: Anti-money laundering.

Arms embargo: prohibit the sale weapons and related services to restricted individuals, groups, or states.

Arrest warrant: An order of a court directing a law enforcement officer to seize and detain a particular person to answer to a complaint or otherwise appear in court.

B

BCBS: Basel Committee on Banking Supervision. This Committee, established by the central bank governors of the G-10 in 1974, promotes sound supervisory standards worldwide. Banking supervisors have a role in ensuring that banks have procedures in place, including management of risks related to money laundering and terrorist financing. One of its papers - Sound management of Risks related to

Money Laundering and Terrorist Financing (2014) - has a few paragraphs on economic sanctions, included in Chapter 6 "Reporting of Suspicious Transactions and Asset Freezing." Paragraph 60 says "A bank should be able to identify and to enforce funds freezing decisions made by the competent authority and it should otherwise not deal with any designated entities or individuals (eg terrorists, terrorist organisations) consistent with relevant national legislation and UNSCRs." Further, paragraph 62 says "All banks should have systems in place to detect prohibited transactions (eg transactions with entities designated by the relevant UNSCRs or national sanctions). See: http://www.bis.org/publ/bcbs275.pdf The Committee's Secretariat is provided by the Bank for International Settlements in Basel, Switzerland. See www.bis.org.

Beneficial owner: Also referred to as "ultimate beneficial owner." Refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

BIS: Bureau of Industry and Security of the US Department of Commerce. Its mission is to advance U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership. BIS implements U.S. government sanctions against Cuba, Iran, North Korea, Sudan, and Syria pursuant to the EAR, either unilaterally or to implement UN Security Council Resolutions. The license requirements, license exceptions, and licensing policy vary depending upon the particular sanctioned destination. The BIS website is a useful resource for information on which destinations are subject to foreign policy related controls.

See:
http://www.bis.doc.gov/index.php/policy-guidance/country-guidance/sanctioned-destinations

Blocking: According to OFAC FAQ on its website, another word for "blocking" is "freezing." It is simply a way of controlling targeted property. Title to the blocked property remains with the target, but the exercise of powers and privileges normally associated with ownership is prohibited without authorization from OFAC. Blocking immediately imposes an across-the-board prohibition against transfers or dealings of any kind with regard to the property.

Blocking Statute: European Union's Council Regulation (EC) No 2271/96 that prohibits EU companies from complying with sanctions that are not imposed by the European Union. The regulation was updated in 2018 in response to U.S. secondary sanctions against Iran.

C

CES: The Counterintelligence and Export Control Section of the US Department of Justice. CES investigates, prosecutes, and supervises the investigation and prosecution of cases affecting the national security and foreign relations of the United States, including espionage cases, cases involving the illegal export of military and strategic commodities and cases involving certain cyber-related activity.

CFSP: Common Foreign and Security Policy of the European Union. EU Member states have committed themselves to a CFSP for the EU. The EU imposes sanctions and embargoes to further its CFSP objectives. So, to influence policies violating international law or human rights, or policies disrespectful of the rule of law or democratic principles, the EU has designed sanctions of a diplomatic or economic nature.

CISADA: The Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010. This act enables the U.S. Treasury to prohibit or impose conditions on opening or maintaining U.S. correspondent banking or payable-through accounts for a non-U.S. financial institution found to knowingly engage in sanctionable activities. This includes those entities that facilitate (i) Iran's WMD acquisition or development, or Iran's support for international terrorism; or (ii) significant transactions or providing significant financial services for designated banks or for Iran's Islamic Revolutionary Guard Corps or its affiliates, which include large commercial enterprises. Since CISADA was signed into law, Treasury has reportedly engaged with over 120 financial institutions and bank regulators in more than 60 countries all over the world to brief them on the financial provisions of CISADA. As a result of this global campaign, many non-U.S. financial institutions changed their business practices – even closed any correspondent accounts with U.S. designated Iranian banks – to ensure that their access to the U.S. financial system is not put at risk. As a result of the sanctions imposed under CISADA, financial institutions may not open correspondent or payable-through accounts for banks designated under CISADA and any financial institutions that currently hold such accounts must close them within 10 days.

Collective knowledge: A legal principle that states that a financial institution or any other corporate entity is in possession of the sum of the knowledge that is held separately by its directors, officers and employees.

Comprehensive sanctions: employ extensive trade embargoes against the target of sanctions and involve wide-sweeping bans on trade, diplomatic relations, and or other relationships between target and sender. For example, sanctions that prohibit the import or export of goods and services that benefit a country or region.

Consolidated Sanctions List: All of OFAC's non-SDN sanctions lists (including the Non-SDN, Palestinian Legislative Council List "NS-PLC List", the Part 561 List, the Non-SDN Iran Sanctions Act List "NS-ISA List", the Foreign Sanctions Evaders List "FSE List", and the Sectoral Sanctions Identifications List "SSI List") are included in a consolidated set of data files "the Consolidated Sanctions List". While the consolidated sanctions list data files are not part of OFAC's list of Specially Designated Nationals and Blocked Persons "the SDN List," the records in these consolidated files may also appear on the SDN List. See https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/consolidated.aspx

Correspondent Banking Due Diligence Questionnaire (CBDDQ): In direct response to increased regulatory expectations for enhanced due diligence in correspondent banking relationships, the Wolfsberg Group published its new Correspondent Banking Due Diligence Questionnaire (CBDDQ) in February 2018, incorporating a number of important changes. The new Questionnaire is not only four times as long as its 2014 predecessor, containing 110 instead of 28 questions, but has also expanded its scope to specifically address due diligence issues relating to Anti-Bribery and Corruption, Counter terrorism Financing and Sanctions exposure controls.

Criminal Complaint: In criminal law, the criminal complaint in many countries is the preliminary charge or accusation made by one against another to the appropriate court or officer, usually a magistrate. In the U.S., criminal proceedings against a person can be instituted by a criminal complaint until an indictment is handed down.

Culture of Sanctions Compliance: For an sanctions compliance program to be effective, it should have demonstrable support from the firm's leadership. Boards of directors and senior management should set the tone for the organization by creating a culture of compliance. To comply with economic sanctions, key personnel should receive ongoing sanctions compliance training and be familiar with requirements and prohibitions and understand the potential impact that violations can have on the firm.

Customer screening: The screening of full legal name and any other name provided by the customer, such as known aliases, against applicable official sanctions lists. Also called name screening.

Cyber Sanctions: These are sanctions directed against persons or entities engaging in activities that threaten the cyber security of the United States, and especially the integrity of the U.S. electoral process. An example is Executive Order 13694 issued by US President Obama, dated April 1, 2015, named "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities." Persons and entities subject to these sanctions are designated as SDNs.

D

DBA: Term used to describe an entity's business or trade name, meaning "doing business as" (such as ABC Corporation, dba John's Autoparts). The term is used in watchlists with sanctioned entities or persons.

DDTC: The Directorate of Defense Trade Controls (DDTC), agency within the U.S. State Department, that administers the exportation of defense articles under the International Traffic in Arms Regulations (ITAR).

Delisting: Lifting of sanctions measures by removing an individual or entity from the relevant sanctions list.

De minimus requirements: Some export prohibitions contain de minimus requirements, so that the prohibition does not apply if the value of the U.S. content of the finished good, service or technology is below a specified percentage.

Designated Person or Entity: According to the Glossary of the FATF Recommendations, this refers to: (i) individual, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1267 (1999) (the 1267 Committee), as being individuals associated with Al-Qaida, or entities and other groups and undertakings associated with Al-Qaida; (ii) individuals, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1988 (2011) (the 1988 Committee), as being associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan, or entities and other groups and undertakings associated with the Taliban; (iii) any natural or legal person or entity designated by jurisdictions or a supra-national jurisdiction pursuant to Security Council resolution 1373 (2001); (iv) any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution 1718 (2006) and its successor resolutions by the Security Council in annexes to the relevant resolutions, or by the "Security Council Committee established pursuant to resolution 1718 (2006)" (the 1718 Sanctions Committee) pursuant to Security Council resolution 1718 (2006); and (v) any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution 1737 (2006) and its successor resolutions by the Security Council in annexes to the relevant resolutions, or by the "Security Council Committee established pursuant to paragraph 18 of resolution 1737 (2006)" (the 1737 Sanctions Committee) pursuant to resolution 1737 (2006) and its successor resolutions.

Designation: According to the FATF Recommendations Glossary, this term refers to the identification of a person or entity that is subject to targeted financial sanctions pursuant to:

- United Nations Security Council resolution 1267 (1999) and its successor resolutions;
- Security Council resolution 1373 (2001), including the determination that the relevant sanctions will be applied to the person or entity and the public communication of that determination;
- Security Council resolution1718 (2006) and its successor resolutions;
- Security Council resolution 1737 (2006) and its successor resolutions; and
- any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction.

Diplomatic sanctions: The reduction or removal of diplomatic ties, such as embassies.

DOJ: United States Department of Justice. See www.usdoj.gov.

Downstream Correspondent Clearer: Defined by the Wolfsberg AML Principles for Correspondent Banking as a correspondent banking client who receives correspondent banking services from an institution and itself provides correspondent banking services to other financial institutions in the same currency as the account it maintains with the institution.

Dual-Use: Dual-use goods and technologies are those which have both civilian and direct military uses. Dual-use goods are typically subject to export controls. The Wassenaar Arrangement has issued a number of documents regarding dual use goods.

E

ECO: Export Control Organisation, part of the UK government's Department for Business, Innovation & Skills. The chief task of the ECO is to process applications for licenses to export strategic goods, software and technology from the UK.

Economic sanctions: The restriction or prohibition of trade and financial relations for foreign policy and national security purposes. Economic sanctions are meant to isolate the target by denying it access to resources. Economic sanctions may include trade embargoes or boycotts, freezing of assets, bans on cash transfers, bans on technology transfer and restrictions on travel.

EEAS: European External Action Service. The EEAS was formally launched in 2011, and is the EU's diplomatic service. It helps the EU's foreign affairs chief – the High Representative for Foreign Affairs and Security Policy – carry out the Union's Common Foreign and Security Policy. Sanctions – also referred to as restrictive measures – against third countries, individuals or entities, are an essential EU foreign policy tool that it uses to pursue objectives in accordance with the principles of the Common Foreign and Security Policy. The EU

Consolidated List is published on the EEAS website http://eeas.europa.eu/cfsp/sanctions/index_en.htm

EFT: Electronic Funds Transfer. The movement of funds through electronic means between financial institutions. The two most common electronic funds transfer systems are FedWire and CHIPS. (SWIFT is often referred to as the third EFT system; in reality it is an international messaging system that carries instructions for wire transfers between banks, rather than the actual wire transfer system itself.) Other systems that facilitate funds movement, but are not technically EFT systems, include automated clearing house, or ACH, networks that conduct batch processing of messages for book transfers between institutions.

Egregious: In case of a violation, OFAC will consider several factors in deciding what action to take. If it decides to impose a penalty (or agree to a negotiated penalty), OFAC will consider in particular whether the conduct was "egregious." In assessing egregiousness, OFAC looks at the following factors:

- Willfulness
- Awareness
- Harm to sanctions objectives
- Individual characteristics

EOUSA: Executive Office of U.S. Attorneys, Department of Justice (DOJ). See www.usdoj.gov.

EU: European Union.

EU Consolidated List: Consolidated list of persons, groups and entities subject to EU financial sanctions. The correct application of financial sanctions is crucial in order to meet the objectives of the EU's Common Foreign and Security Policy and especially to help prevent the financing of terrorism. The application of financial sanctions constitutes an obligation for both the public and private sector. In this regard, the EU assigns particular responsibility to credit and financial institutions, since they are involved in the bulk of financial transfers and transactions affected by the relevant regulations. In order to facilitate the application of financial sanctions, the European Banking Federation, the European Savings Banks Group, the European Association of Co-operative Banks and the European Association of Public Banks ("the EU Credit Sector Federations") and the Commission recognized the need for an EU consolidated list of persons, groups and entities subject to CFSP related financial sanctions. It was therefore agreed that the Credit Sector Federations would set up a database containing the consolidated list for the Commission, which would host and maintain the database and keep it up-to-date. This database was developed first and foremost to assist the members of the EU Credit Sector Federations in their compliance with financial sanctions. See: http://eeas.europa.eu/cfsp/sanctions/consol-list/index_en.htm

Executive order: The immediate legal authority for the imposition of sanctions in the United States usually takes the form of an Executive Order issued by the President. While an Executive Order must be based on power delegated to the President by a statute, Congress does not review or approve Executive Orders (although it can overturn them by statute). As a consequence, the President can interpret, modify, and withdraw Executive Orders without any action by Congress. As a practical matter, most U.S. sanctions are imposed pursuant to an Executive Order.

Export controls: Controls countries place on exports of goods, services, and technology. The United States and the EU, among others, restrict the export of defense items or munitions; so-called "dual-use" goods and technology; certain nuclear materials and technology; and items that would assist in the development of nuclear, chemical, and biological weapons or the missile technology used to deliver them.

Extradition: The surrender by one country to another of an accused or convicted person under a bilateral agreement that specifies the terms of such exchanges, the persons subject to being exchanged and the crimes for which exchanges will be permitted. The 1988 Vienna Convention provides for money laundering to be an internationally extraditable offence.

Extraterritorial sanctions: Traditionally, unilateral sanctions prohibit only a home country's or region's corporations and citizens from doing business with a blacklisted entity. However, extraterritorial sanctions restrict the economic activity of governments, businesses, and nationals of third countries. As result, governments typically consider these sanctions a violation of sovereignty and international law. These are sometimes called secondary sanctions.

F

Facilitation: Facilitation provisions under U.S. sanctions programs are measures that make it an offense for any U.S. person to approve, facilitate, guarantee or finance any transaction by a foreign person where the transaction by that foreign person would be prohibited if performed by the US person.

FFC: Office of Foreign Funds Control, the predecessor of OFAC. FCC was established at the advent of World War II following the German invasion of Norway in 1940. The FFC program was administered by the US Secretary of the Treasury throughout the war. The FFC's initial purpose was to prevent Nazi use of the occupied countries' holdings of foreign exchange and securities and to prevent forced repatriation of funds belonging to nationals of those countries. These controls were later extended to protect assets of other invaded countries. After the United States formally entered World War II, the FFC played a leading role in economic warfare against the Axis powers by blocking enemy assets and prohibiting foreign trade and financial transactions.

FFIEC Bank Secrecy Act/Anti Money Laundering Examination Manual (2014): Provides guidance for examiners when conducting BSA/AML examinations at financial institutions. The Manual has a section on sanctions, and refers to sanctions several times.

Financial Action Task Force (FATF): An independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognized as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard. The FATF is also referred to by its French or Spanish acronym, GAFI, or Grupo de Acción Financiera Internacional. See: www.fatf-gafi.org.

FATF Recommendations: Officially called The International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, these recommendations issued by the FATF set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. There are several recommendations that cover issues related to sanctions: Recommendation 6 covers targeted financial sanctions related to terrorism and terrorist financing. Recommendation 7 covers targeted financial sanctions related to proliferation.

FBI: Federal Bureau of Investigation, an investigative agency within the U.S. Department of Justice.

FCA: Financial Conduct Authority of the United Kingdom. The Financial Conduct Authority is the conduct regulator for 59,000 financial services firms and financial markets in the UK and the prudential regulator for over 18,000 of those firms. Integrity of the UK's financial markets requires the FCA to ensure firms have effective systems and controls to detect, prevent and deter financial crime.

FIU: Financial Intelligence Unit. An intelligence-gathering law enforcement or regulatory body that receives financial information from the covered financial institutions, businesses and persons in its respective country. Generally, it analyzes and processes the information and disseminates it to appropriate government authorities in support of anti-money laundering efforts and financial crimes investigations. Sometimes the term Financial Investigative Unit is used, in addition to Financial Intelligence Unit. See Egmont Group.

Focal Point For De-Listing: Focal Point in the United Nations that receives and processes requests from individuals and entities seeking removal from all UNSC sanctions lists except for the ISIL (Da'esh) and Al-Qaida Sanctions List, which is dealt with by the Office of the Ombudsperson. In accordance with the Focal Point's procedures, the decision to de-list rests solely with the relevant sanctions committee. The Focal Point also receives travel ban and assets freeze exemption requests in relation to individuals and entities on the ISIL (Da'esh) and Al-Qaida and the 1988 Sanctions Lists. Finally, the Focal Point also receives communications from individuals removed from the ISIL (Da'esh) and Al- Qaida Sanctions List and those claiming to have been mistakenly subjected to the sanctions measures pursuant to that List.

Foreign Sanctions Evaders (FSE) List: OFAC publishes a list of foreign individuals and entities determined to have violated, attempted to violate, conspired to violate, or caused a violation of U.S. sanctions on Syria or Iran. It also lists foreign persons who have facilitated deceptive transactions for or on behalf of persons subject to U.S. sanctions. Collectively, such individuals and companies are called "Foreign Sanctions Evaders" or "FSEs." Transactions by U.S. persons or within the United States involving FSEs are prohibited. Click here for a list of frequently asked questions on Foreign Sanctions Evaders, including information on dealings with FSEs. The FSE List is not part of the Specially Designated Nationals (SDN) List. However, individuals and companies on the FSE List may also appear on the SDN List. See: https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/fse_list.aspx

Forfeiture: The permanent loss of property or assets by legal action by a government authority for failure to comply with the law or for the involvement of the property in a criminal activity.

Framework for OFAC Compliance Commitments: A 2019 source of guidance issued by OFAC for any organization doing business with the United States, including selling into the United States, selling U.S. products, purchasing U.S. products, or even simply using U.S. dollars. The guidance, in many ways represents a distillation of international best practices related to sanctions compliance. In this document, OFAC has identified five major components of sanctions compliance program:

1. Management commitment
2. Risk assessment
3. Internal controls
4. Testing and auditing
5. Training

Freeze of economic resources: Preventing owners of economic resources from utilizing them by placing funds and other assets in special accounts, etc. This term also includes preventing their use to obtain funds, goods, or services in any way, including, but not limited to, by selling, hiring o mortgaging them.

Freezing: See blocking.

FTO: Foreign Terrorist Organization. These are foreign individuals or entities found to have committed, or which pose a significant risk of committing, acts of terrorism that threaten US national security, foreign policy, or its economy. Legally, the effect of designation, by U.S. Department of State, as an FTO is similar to that for designation as an SDN.

Funds: According to the FATF Recommendations Glossary, this term refers to assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets.

Funds or other assets: According to the FATF Recommendations Glossary, this term means any assets, including, but not limited to, financial assets, economic resources, property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travelers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.

Fuzzy matching: a varied and algorithm based technique to one name (a string of words), where the contents of the information being screened is not identitical, but is spelling, pattern or sound is a close match to the contents contained on a list used for screening.

G

GAFI: Grupo de Accion Financiera Internacional, or Groupe d'action financière sur le blanchiment de capitaux. Spanish and French term for Financial Action Task Force, or FATF.

GAFISUD: South American Financial Action Task Force, created in December 2000, in Cartagena, Colombia. Its main objective is to implement anti-money laundering and counter terrorism financing measures in South America. See www.minjusticia.gov.co/gafisud

GAO: The United States General Accounting Office. It is the investigative arm, or watchdog, of the U.S. Congress. The GAO has issued several reports related to sanctions. Members of Congress and Congressional committees can commission the GAO to undertake a study or review of an issue. For a list of the GAO publications and reports, see www.gao.gov.

H

HM Treasury: United Kingdom government's economic and finance ministry. It maintains control over public spending, sets the direction of the UK's economic policy and works to achieve strong and sustainable economic growth. HM Treasury is also responsible for the implementation and administration of international financial sanctions in effect in the UK, for domestic designations under the Terrorist Asset-Freezing etc. Act (TAFA) 2010, licensing exemptions to financial sanctions, and directions given under Schedule 7 to the Counter-Terrorism Act 2008, and under Council Regulation (EU) No.833/2014, concerning Russia's actions in Ukraine. https://www.gov.uk/guidance/sanctions-embargoes-and-restrictions

I

IEEPA: International Emergency Economic Powers. Codified at Title 50 U.S.Code Sec. 1701, gives the U.S. President the ability to impose economic and other sanctions where he declares (by Executive Order) that there is an "unusual and extraordinary threat" to the United States. The IEEPA has been used to sanction (and invade) Iraq, sanction Iran, Syria, and other nations, and to sanction drug traffickers and terrorists and terrorist organizations. IEEPA is a key underlying authority for OFAC sanctions.

IMO number: A unique seven-digit number on a maritime vessel. Maritime vessels are required to display their name and International Maritime Organization (IMO) number in a visible location. A vessel's IMO number is intended to be permanent regardless of a change in a vessel's ownership or name. This allows for identification of the vessel itself. Sanctions evaders may obscure the IMO number, or even change it illegally, to disguise the connection of the vessel to a country subject to sanctions, such as North Korea.

INSTEX: Instrument in Support of Trade Exchanges. Payment channel, or Special Purpose Vehicle created by Germany, France and the U.K. in 2019 to facilitate ongoing trade with Iran as per the terms of the JCPOA. Currently, mainly used for humanitarian purposes (food, medicine). System that acts a middle man, or mirror-trading transaction system.

International Best Practices: Targeted Financial Sanctions related to Terrorism and Terrorist financing (recommendation 6): Report issued by the FATF in 2013 that covers Recommendation 6 of the FATF Recommendations. It sets out non-binding guidance based on updates in relevant UNSCRs and in response to challenges faced by countries in the implementation of the requirements of Recommendation 6. It explains the importance of an effective freezing regime, and includes best practices for procedures on identifying, designating and delisting of persons or entities, reviewing, freezing and unfreezing, and compliance and access to frozen funds or other assets.

Indictment: Term used in several countries, including the U.S., for a formal written accusation, drawn up and submitted to a Grand Jury by the prosecutor, charging one or more persons with a crime upon a majority vote of the grand jurors.

Intermediary Financial Institution: A financial institution that receives funds from a wire transfer transmitter's financial institution and relays or transmits the order of payment to the recipient's financial institution. In an international funds transmission, these institutions are often located in different countries. The originating and beneficiary institutions do not have a direct relationship and need to "relay" the wire transfer through an institution or institutions that have relationships with the previous bank. For example, a customer at Bank A in the United States may want to send funds to a customer at Bank X in Germany. If banks A and X have no direct relationship, Bank A might first route the wire through Bank B in the United States, which in turn has a relationship with Bank Y in Germany, which then routes it to the beneficiary Bank, Bank X. In this case, Bank A is the originating bank, Banks B and Y are intermediary banks, and Bank X is the beneficiary bank.

Interpretive guidance: OFAC issues interpretive guidance on specific issues related to the sanctions programs it administers. These interpretations of OFAC policy are sometimes published in response to a public request for guidance or may be released proactively by OFAC in order to address a complex topic. The guidance is typically placed in the "Resource Center" on the OFAC website, See: https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/rulings-index.aspx

ITAR:_International Traffic in Arms Regulations. These U.S. regulations apply specifically to defense articles, which include hardware and software technology, as well as services that may be used militarily, such as certain space-related items and technology. The ITAR contains the US Munitions List, which is a comprehensive list of all defense articles and services subject to ITAR and controlled by the DDTC.

ITRS: The Iran Threat Reduction and Syria Human Rights Act of 2012 (Public Law 112–158 was enacted on August 10, 2012. It amended ISA to add new criteria for the imposition of secondary sanctions on persons doing business in Iran's energy and weapons sectors. It authorized additional sanctions against persons who conduct certain business with NIOC and NITC, similar to Executive Order 13622, but with a focus on underwriting and insurance services; and authorizes sanctions for the purchase, subscription to, or facilitation of the issuance of Iranian sovereign debt or the debt of any entity owned or controlled by the government of Iran. There are Iran-related disclosure requirements for securities issuers, including those that are not based in the U.S., and secondary sanctions even on agencies of third-country governments that knowingly provide financial support or services to designated IRGC affiliates.

J

JCPAO: Joint Comprehensive Plan of Action. China, France, Russia, the United Kingdom, and -previously- United States—the five permanent members of the UN Security Council—negotiated the agreement alongside Germany; together they were known as the P5+1. Iran and the P5+1 reached a plan related to sanctions relief on July 14, 2015. The plan provides phased sanctions relief following the

IAEA verification that Iran has taken its nuclear related steps. The United States' withdrawal in May 2018 from the agreement has heightened tensions and left the remaining signatories scrambling to keep the deal alive.

JCPOA Full Text, Annexes, and Attachments:
http://www.state.gov/e/eb/tfs/spi/iran/jcpoa/index.htm

K

Kingpin Act: On December 3, 1999, the U.S. President signed into law the Kingpin Act (21 U.S.C. §§ 1901-1908 and 8 U.S.C § 1182), providing authority for the application of sanctions to significant foreign narcotics traffickers and their organizations operating worldwide. The Kingpin Act which was enacted into law as part of the Intelligence Authorization Act for Fiscal Year 2000. Modeled on the successful application of economic sanctions in 1995 against the Cali narcotics cartel in Colombia' pursuant to IEEPA, the Kingpin Act provides for the imposition of economic sanctions on a world-wide basis against major international narcotics traffickers, their organizations, and the foreign individuals and entities that provide support for those traffickers and their organizations.

KYC: Know Your Customer or Know Your Client. The term used to describe a set of financial crime control policies and procedures that are used to determine the true identity of a customer/client and the type of activity that will be "normal and expected" for the customer, and to detect activity that should be considered "unusual" for the particular customer.

KYCB: Know Your Correspondent Bank. The term used to describe a set of money laundering control policies and procedures used to determine the beneficial owners of a respondent bank and the type of activity that will be "normal and expected" for this bank. Know Your Correspondent Bank is a key tool in detecting suspicious activity and money laundering activity because correspondent accounts are often used as conduits to launder criminal proceeds in international settings. The USA PATRIOT Act of 2001 enacted a number of statutory provisions that bear directly on the procedures U.S. financial institutions must follow in connection with their foreign correspondent banks.

L

Letter of Credit (LC): A letter of credit is a credit instrument issued by a bank guaranteeing payments on behalf of its customer to a third party when certain conditions are met. LCs are commonly used to finance exports. The exporters want assurance that the ultimate buyer of its goods will make payment, an assurance given by the buyer's purchase of a bank letter of credit. The LC is then forwarded to a correspondent bank in the city in which the payment is to be made. The LC is drawn on when the goods are loaded for shipping, received at the importation point, clear Customs, and they are delivered, etc. LCs can be used to facilitate money laundering by transferring money from a country with exchange controls, thus assisting in creating the illusion that an import transaction is involved. According to several OFAC enforcement actions, sometimes financial institutions amend or delete OFAC-listed names or countries in LCs to avoid detection by OFAC filters.

License: A license is an authorization from a government agency such as OFAC to engage in a transaction that otherwise would be prohibited. There are two types of licenses: general licenses and specific licenses. A general license authorizes a particular type of transaction for a class of persons without the need to apply for a license. A specific license is a written document issued by OFAC to a particular person or entity, authorizing a particular transaction in response to a written license application. Persons engaging in transactions pursuant to general or specific licenses must make sure that all conditions of the licenses are strictly observed. OFAC's regulations may contain statements of OFAC's specific licensing policy with respect to particular types of transactions.

Lista Clinton: Spanish for “Clinton list.” Term sometimes used in Latin America when referring to the Specially Designated Narcotic Traffickers List, which identifies persons and entities whose assets must be blocked by any U.S. person who controls them. The list is administered by the U.S. Treasury Department’s Office of Foreign Assets Control (OFAC). It was initiated by Executive Order of President Bill Clinton in October 1995.

M

Magnitsky Act: In 2012, the violent death of Russian whistleblower, Sergei Magnitsky, in a Russian prison gave rise to the U.S. Magnitsky Act, a piece of legislation (Public Law 112-208) allowing the U.S. government to impose targeted sanctions against Russian individuals involved in human rights violations related to his death. Executive Order 13818 implements the provisions of the Global Magnitsky Act. As a result of designations pursuant to the E.O., all of the property and interests in property within U.S. jurisdiction of the designated individuals and entities are blocked, and U.S. persons are generally prohibited from engaging in transactions with them.

Military sanctions: Military intervention.

MLAT: Mutual Legal Assistance Treaty. A treaty that is usually between two countries that allows for mutual assistance in legal proceedings and access to documents and witnesses and other legal and judicial assistance in the respective countries from private and public sources for use in official investigations and prosecutions.

MLCA: The Money Laundering Control Act of 1986, codified at Title 18, U.S. Code Section 1956. The MLCA was the first law in the world to make money laundering a crime. It is one of the most powerful anti-money laundering laws in the world. The MLCA applies to the proceeds of some 200 underlying or predicate crimes (called Specified Unlawful Activities, or SUAs), including several sanctions violations (e.g, criminal violations in Title 50 (IEEPA)), and imposes heavy penalties – up to 20 years in prison. It has extraterritorial reach if the offence is committed by a U.S. citizen or by a non-U.S. citizen whose conduct "occurs in part" in the U.S. and if the transaction involves more than $10,000. Among the primary offences in Section 1956 is knowingly engaging in a financial transaction with proceeds of an SUA or with the intent to conceal the true source of ownership of the proceeds or in order to avoid the mandatory reporting requirements. Section 1956 was substantially amended by the USA PATRIOT Act.

MOU: Memorandum of Understanding. An agreement between two parties establishing a set of principles within which they will govern their relationship on a particular matter. MOUs are used by countries to govern their sharing of assets in international asset-forfeiture cases or to set out their respective duties in anti-money laundering initiatives. MOUs are also used between U.S. government agencies on the sharing of information between themselves. Examples are agreements signed between OFAC and the IRS, and federal banking regulators with respect to reviews conducted by the IRS or the regulator for compliance with U.S. economic sanctions. The sharing of information under such MOUs is intended to help OFAC in administrating U.S. economic sanctions and to assist the banking regulators and IRS in exercising its delegated examination authorities.

Multilateral sanctions: Sanctions agreed upon between multiple countries. UN sanctions are by definition multilateral sanctions.

N

NDDA: The National Defense Authorization Act for Fiscal Year 2012. This Act includes a new authority to impose secondary sanctions on non-U.S. banks. Signed into law on December 31, 2011, the NDAA essentially replicates CISADA's focus on transactions with designated banks but adds the Central Bank of Iran as a new criterion for sanctions. It also includes a unique provision for "exceptions" to the sanctions: If the president finds that a country made significant reductions in Iranian crude oil purchases, then that country's financial institutions can receive a 180-day exception from sanctions under the NDAA — even if they otherwise meet the criteria for such sanctions.

Non-economic sanctions: These include:

- Canceling ministerial and summit meetings with a target country;
- Denying a target country's government officials visas to enter the sender country;
- Withdrawing a sender country's ambassador or otherwise downgrading diplomatic and military contacts with a target country;
- Blocking a target country from joining international organizations;
- Opposing a target country's bid to host highly visible international events, such as the Olympics;

- Withholding foreign aid; and
- Instructing a sender country's directors to vote against new loans to a target country at the World Bank or other international financial institutions.

Non-SDN Iranian Sanctions Act: On May 23, 2011, President Obama signed Executive Order ("E.O.") 13574, "Authorizing the Implementation of Certain Sanctions Set Forth in the Iran Sanctions Act of 1996, as Amended." E.O. 13574 states that the Secretary of the Treasury, pursuant to authority under the International Emergency Economic Powers Act ("IEEPA"), shall implement certain sanctions that the Secretary of State imposes and selects under the pre-existing authority of the Iran Sanctions Act of 1996 ("ISA") as amended by the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 ("CISADA"). See: https://www.treasury.gov/resource-center/sanctions/Programs/Pages/iran.aspx#part561

NSD: National Security Division of the US Department of Justice. The mission of the NSD is to coordinate the Department's efforts in carrying out its core mission of combating terrorism and protecting national security. NSD is responsible for supervising the enforcement of all federal criminal laws related to counterterrorism and counterespionage, except those specifically assigned to other divisions. NSD also serves as the Department of Justice's liaison to the United States Intelligence Community (USIC) and represents the government and the USIC before the Foreign Intelligence Surveillance Court. NSD advises the Attorney General regarding all matters of national security policy.

O

OFAC: The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under US jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

OFAC fine: OFAC can impose hefty fines for violations of sanctions programs. Depending on the program, criminal penalties for willful violations can include fines ranging up to $20 million and imprisonment of up to 30 years. Civil penalties for violations of the Trading With the Enemy Act can range up to $65,000 for each violation. Civil penalties for violations of the International Emergency Economic Powers Act can range up to $250,000 or twice the amount of the underlying transaction for each violation. Civil penalties for violations of the Foreign

Narcotics Kingpin Designation Act can range up to $1,075,000 for each violation. Potential criminals violations may be referred to the Department of Justice.

OFAC 50% Rule: Entities that a person on the OFAC 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. In August 2014, OFAC issued revised guidance "Revised guidance on entities owned by persons whose property and interest are blocked" (see: https://www.treasury.gov/resource-center/sanctions/Documents/licensing_guidance.pdf) that says that the property and interests in property of entities directly or indirectly owned 50 percent or more in the aggregate by one or more blocked persons are considered blocked regardless of whether such entities appear on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) or the annex to an Executive order. The revised guidance expands upon the earlier guidance by setting forth a new interpretation addressing entities owned 50 percent or more in the aggregate by more than one blocked person. U.S. persons are advised to act with caution when considering a transaction with a non-blocked entity in which one or more blocked persons has a significant ownership interest that is less than 50 percent or which one or more blocked persons may control by means other than a majority ownership interest. Such entities may be the subject of future designation or enforcement action by OFAC. Furthermore, a U.S. person may not procure goods, services, or technology from, or engage in transactions with, a blocked person directly or indirectly (including through a third- party intermediary).

Office of the Ombudsman of the Al-Qaida Sanctions Committee: An independent and impartial Ombudsperson, who reviews requests from individuals, groups, undertakings or entities seeking to be removed from the Al-Qaida Sanctions List of the UN Security Council's Al-Qaida Sanctions Committee. See: https://www.un.org/sc/suborg/en/ombudsperson

OFSI: As of March 2016, the United Kingdom has created the Office of Financial Sanctions implementation (OFSI) (replacing the HM Treasury's Asset Freezing Unit), which is responsible for the implementation and administration of international financial sanctions in the UK. The Department for Business, Innovation & Skills (BIS) is responsible for trade sanctions. The OFSI, a part of Her Majesty (HM)'s Treasury Department of the U.K. government, is the authority for the implementation of financial sanctions in the U.K.

P

Palestinian Legislative Council (PLC) list: List issued by OFAC. This list is NOT part of the Specially Designated Nationals [SDN] List). Section (b) of General License 4 issued pursuant to the Global Terrorism Sanctions Regulations (31 C.F.R. Part 594), the Terrorism Sanctions Regulations (31 C.F.R. Part 595), and the Foreign Terrorist Organizations Sanctions Regulations (31 C.F.R. Part 597) authorizes U.S. financial institutions to reject transactions with members of the

Palestinian Legislative Council (PLC) who were elected to the PLC on the party slate of Hamas, or any other Foreign Terrorist Organization (FTO), Specially Designated Terrorist (SDT), or Specially Designated Global Terrorist (SDGT), provided that any such individuals are not named on OFAC's list of Specially Designated Nationals and Blocked Persons (SDN List). See: https://www.treasury.gov/resource-center/sanctions/Terrorism-Proliferation-Narcotics/Pages/index.aspx

Part 561 List: In order to implement certain provisions of the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA), the National Defense Authorization Act of Fiscal Year 2012 (NDAA), the Iran Freedom and Counter-Proliferation Act of 2012 (IFCA) and certain executive orders, OFAC has developed a list of foreign financial Institutions that are subject to sanctions under these laws and orders. See: https://www.treasury.gov/resource-center/sanctions/Programs/Pages/iran.aspx#part561

Presumption of denial policy: A term used in license review policy at U.S. agencies, for example at the Department of Commerce, BIS. For example, on August 2018, Department of Commerce Bureau of Industry and Security (BIS) issued 15 CFR Part 744 “Addition of Certain Entities; and Modification of Entry on the Entity List”. This rule amends the Export Administration Regulations (EAR) by adding 44 entities to the Entity List. The rule says “For all forty-four entities added to the Entity List in this final rule, BIS imposes a license requirement for all items subject to the EAR, and a license review policy of presumption of denial” It means you can apply for a license to do business with organizations on the Entity List, but it is it is very likely that BIS will not grant that license.

Policies: Internal “rules” of a financial institution that define how employees are expected to conduct themselves and the operating rules of the financial institution or business. Policies, including sanctions compliance policies, are general statements of intent and action, generally requiring implementing procedures.

Predicate Crimes: Most money laundering laws contain a wide definition or listing of predicate crimes or Specified Unlawful Activities whose proceeds, if involved in the subject transaction, can give rise to prosecution for the crime of money laundering. Sometimes, the predicate crimes are defined as “felonies” or “all offences in the criminal code. In the MLCA, several sanctions violations are considered predicate crimes, including the criminal violations in Title 50 (IEEPA).

Prohibited transactions: OFAC defines prohibited transactions as trade or financial transactions and other dealings in which U.S. persons may not engage unless authorized by OFAC or expressly exempted by statute. Because each program is based on different foreign policy and national security goals, prohibitions may vary between programs.

Proliferation financing: In general, this refers to raising cash, mostly foreign exchange revenue, for proliferators to develop nuclear, ballistic and weapons of mass destruction. Proliferation is not merely about transporting proliferation-related components to regimes like the DPRK but is also linked to the exploitation of strategic goods and technology by the regime to generate revenue. As sanctions have tightened around regimes such as the DPRK, tactics to evade sanctions have evolved and become more reliant on its misuse of legitimate global networks. For example, a recent UN Panel of Experts Report (UN Security Council 1718 Committee, 5 March 2019) referred to a trend of increasingly sophisticated cyberattacks carried out by the DPRK to illegally force the transfer of funds from financial institutions and cryptocurrency exchanges. In 2018, the FATF issues guidance on counter proliferation financing and the implementation of UNSC resolutions to counter the proliferation of WMD.

Property: According to the FATF Recommendations Glossary, this means assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.

Q

...

R

Regulatory Agency: An agency created by a government to supervise and oversee a class of institutions in the domestic economy. A regulatory agency generally has the power to issue regulations, perform audits and examinations, impose fines and penalties, and terminate charters or curtail activities of institutions under its jurisdiction. In the US, some financial regulatory agencies play a role in sanctions compliance: OFAC signs MOUs with these agencies with respect to sanctions compliance. OFAC is not, however, itself a regulatory agency.

Respondent Bank: Any foreign bank for which a domestic bank establishes, maintains, administers or manages a correspondent account.

Restrictive Measures: Official terms for sanctions in the European Union. Restrictive measures against third countries, individuals or entities, are an essential EU foreign policy tool that it uses to pursue objectives in accordance with the principles of the Common Foreign and Security Policy (CFSP). Certain EU measures are imposed by Resolutions adopted by the UN Security Council under Chapter VII of the UN Charter. The EU may however decide to apply autonomous measures in addition to the UN's measures or adopt restrictive measures autonomously. In general terms, the EU imposes its restrictive measures to bring about a change in policy or activity by the target country, part of a country, government, entities or individuals. They are a preventive, non-punitive, instrument which should allow the EU to respond swiftly to political challenges and developments. See: http://eeas.europa.eu/cfsp/sanctions/index_en.htm

S

Sanctions Risk Assessment: Firms should assess potential sanctions risk exposure not only across the entire organization but also in dealings with business partners such as vendors and suppliers. Given the ever-changing nature of OFAC, UN, EU and other countries' sanctions and freeze lists, a company's sanctions risk profile may also change. Firms should revise policies and procedures based on those regions in which it conducts business. Risk assessment can include inherent, perceived and residual risks associated with given business activities and/or relationships in sanctioned jurisdictions or with potentially sanctions entities. For example, how should a firm adjust its operations in light of sanctions against Russia or easing of sanctions against Cuba? Some governments mandate that adequate risk assessments form the core of any sanctions compliance program and that such assessments be tailored to the company's operations and third-party relationships.

SCAD: UN Security Council Affairs Division. SCAD assists the UN Security Council in carrying out its critical responsibilities. SCAD also supports subsidiary bodies established by the Security Council, particularly UN sanctions committees and working groups. A key part of this support comprises the establishment of Expert Groups and identification of suitable candidates to serve on these groups who assist Committees in overseeing sanctions regimes, the so-called SCAD Roster of Experts. Experts are required to have technical skills to assist the relevant Committees/working groups with: (1) Analysis and monitoring of sanctions measures, (2) Investigate incidents of non-compliance, (3) Fact and information gathering, (4) Draft substantive reports on their findings, (4) Make recommendations to the respective committees, (5) Other tasks as required by Security Council resolutions specific to the respective Committees/working groups. See: https://www.un.org/sc/suborg/en/sanctions/expert-roster

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 are generally prohibited from dealing with them. See: https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/
default.aspx

SEC: Securities and Exchange Commission, an independent regulatory agency in the United States that regulates the securities markets. Section 219 of ITRA added a subsection (r) to Section 13 of the Securities and Exchange Act of 1934, requiring issuers to disclose in their reports filed on Forms 10-K, 10-Q, and 20-F certain types of activities involving Iran or certain so-called bad actors during the period covered by the filing. Section 13(r) also requires that issuers concurrently file a separate type of notice with the SEC — which the SEC has designated as IRANNOTICE — identifying the issuer and indicating that it disclosed sanctionable activity in its 10-K, 10-Q, or 20-F.

Section 1956: The section number in the U.S. Code in Title 18 that is called "Laundering of Monetary Instruments," the principal money laundering law of the United States. Introduced as one of two primary sections of the Money Laundering Control Act (MLCA) of 1986, it has been amended multiple times over the years, including amendments contained in the USA PATRIOT Act. Among other things, Section 1956, in general, prohibits anyone knowingly engaging in a financial transaction with illicit proceeds (proceeds of a Specified Unlawful Activity) or with the intent to conceal the true source or ownership of the proceeds or in order to avoid the mandatory reporting requirements. SUAs include several sanctions violations (e.g criminal violations in Title 50 (IEEPA)).

Sectoral sanctions: Target a specific industry of a country or region.

Sectoral Sanctions Identifications (SSI) List: OFAC publishes a list to identify persons operating in sectors of the Russian economy identified by the Secretary of the Treasury pursuant to Executive Order 13662. Directives found within the list describe prohibitions on dealings with the persons identified. See https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/ssi_list.aspx. These sectoral sanctions bring special challenges. They prohibit transactions of or dealings with new debt of longer than 90 days' maturity or with new equity with those listed on the SSI List. Firms should be mindful of OFAC's definition of debt and of the necessity to evaluate transactions for potential violations of the sectoral sanctions, especially, for financial institutions, in the context of trade financing given the inclusion of letters of credit and the extension of credit. Last, firms may need to reevaluate their existing due diligence efforts with clients or entities that may be affected by the new sectoral sanctions or if clients or entities have been added to the SDN list. Prohibitions may not be limited to named persons or entities but may include entities that are 50% or more (OFAC 50% rule) owned by the SDN-listed persons or entities. Consequently, it may be prudent for companies to observe those individuals or entities being targeted for sanctions and ensure they are not owned or controlled by SDNs.

Seize: According to the FATF Recommendations Glossary, this term means to prohibit the transfer, conversion, disposition or movement of property on the basis of an action initiated by a competent authority or a court under a freezing mechanism. However, unlike a freezing action, a seizure is effected by a mechanism that allows the competent authority or court to take control of specified property. The seized property remains the property of the natural or legal person(s) that holds an interest in the specified property at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized property.

Self-disclosure: According to the OFAC FAQ on its website, a company can and is encouraged to voluntarily disclose a past violation. Self-disclosure is considered a mitigating factor by OFAC in Civil Penalty proceedings. A self-disclosure should be in the form of a detailed letter, with any supporting documentation, to Compliance and Enforcement Division, Director, Office of Foreign Assets Control, U.S. Department of the Treasury, 1500 Pennsylvania Ave., N.W., Washington, DC 20220. OFAC does not have an "amnesty" program. The ramifications of non-compliance, inadvertent or otherwise, can jeopardize critical foreign policy and national security goals. OFAC does, however, review the totality of the circumstances surrounding any violation, including the quality of a company's OFAC compliance program.

Ship-to-ship transfers: Transferring of cargo from one ship to another while at sea rather than while in port. This can be related to sanctions evasion. However, there are also legitimate reasons for ship-to-ship transfers. Ships like oil tankers and gas carriers carry huge amount of cargo in bulk which does not have to be unloaded in just one port but at different ports. Or some carriers which are massive in size do not berth (park) in port or jetty for discharge operation due to draught restrictions. In such condition ship to ship transfer is utilized. Further, a ship-to-ship-transfer becomes very economical as a ship does not have to berth at the jetty, especially for large oil tankers, which removes the port berthing charges and also cut short the time for berthing and mooring.

Special Notice: The INTERPOL-United Nations Security Council Special Notice combines the UN sanctions regime with INTERPOL's well-established notice system into an effective law enforcement tool. Special Notices are issued for individuals and entities that are subject to sanctions imposed by the United Nations Security Council. Its principal function is to alert national law enforcement authorities that at least form of sanctions apply. For more information, see https://www.interpol.int/en/How-we-work/Notices/INTERPOL-United-Nations-Security-Council-Special-Notices.

SPI: See: U.S. Department of State Office of Economic Sanctions Policy and Implementation.

SPIRE: The UK government's (Export Control Commission) online export licensing system. Using SPIRE, firms can apply for an export or trade licence for their activities and items if they require a licence for the wide range of "strategic" goods (such as security items, military goods, civilian products designed with a military use or purpose, firearms, police and paramilitary goods, radioactive sources and more). Firms can also use SPIRE to make a Ministry of Defence Form 680 application, Private Venture security grading or Exhibition Clearance applications. See https://www.spire.trade.gov.uk/spire/fox/espire/LOGIN/login.

Sport sanctions: Preventing one country's people and teams from competing in international events.

SSI List: See Sectoral Sanctions Identifications (SSI) List.

State Department's Directorate of Defense Trade Controls: The agency within the U.S. State Department responsible for licensing exports of defense articles and enforcing U.S. export controls with respect to weapons and other military items.

Sting Operation: An investigative tactic in which undercover officers pose as criminals, sometimes through a "front" business, to win the confidence of the targets of the investigation and gather information and obtain evidence of their criminal conduct.

Stripping: A basic way of evading screening where information from a message that would reveal the presence of a sanctioned party is deleted. "Stripping" is the deliberate act of deleting or changing information from payment messages or instructions. This makes it more difficult to identify payments or to connect them to sanctioned parties, individuals or countries. To counteract this, banks will typically reject transactions where fields in a message are left blank.

SUA: Specified Unlawful Activity. A legal term used in the U.S. money laundering laws (See MLCA) that refers to crimes that generate money or profits and whose proceeds can trigger money laundering charges under these laws. Currently, there are approximately 200 SUAs that can serve as a predicate offence for a money laundering prosecution. SUAs include several sanctions violations (e.g criminal violations in Title 50 (IEEPA)).The list of SUAs is set out in Title 18, Section 1956 of the United States Code.

Subpoena: A compulsory legal process or writ issued by a court or other legal body (such as an American Congressional committee) to compel the appearance of the person served with the subpoena, or the production of documents specified in the subpoena at a judicial proceeding, before a grand jury, or before the Congressional Committee. The term is Latin for "under penalty" as the failure to appear or produce documents as set out in the subpoena can expose the recipient to penalties, including contempt of court.

T

Targeted financial sanctions: According to the FATF Recommendations Glossary, this term covers both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities. Targeted sanctions are also sometimes referred to as list-based sanctions. They target specific individuals and entities of a country or a region.

TEC: Treaty Establishing the European Community. The Treaty of Rome, the original full name of which was the Treaty establishing the European Economic Community (TEEC). It has been amended by successive treaties, changing its content, including by the 1992 Treaty of Maastricht, which established the European Union with the EEC becoming one of its three pillars, the European Community. Hence, the Treaty was then renamed the Treaty Establishing the European Community. When the Treaty of Lisbon came into force in 2009, the pillar system was abandoned, and the EC ceased to exist as a legal entity separate from the EU. The treaty was amended again, and renamed the Treaty on the Functioning of the European Union (TFEU). The Treaty of Lisbon upgraded the European Union's treaty provisions against oppressive third countries, dictators and their henchmen as well as their foreign assets, by amongst others, inserting a new Title IV on restrictive measures, containing Article 215 TFEU, which brought economic and financial sanctions against third countries under one roof, combining Articles 301 and 60(1) TEC:

TITLE IV

RESTRICTIVE MEASURES

Article 215

(ex Article 301 TEC)

1. Where a decision, adopted in accordance with Chapter 2 of Title V of the Treaty on European Union, provides for the interruption or reduction, in part or completely, of economic and financial relations with one or more third countries, the Council, acting by a qualified majority on a joint proposal from the High Representative of the Union for Foreign Affairs and Security Policy and the Commission, shall adopt the necessary measures. It shall inform the European Parliament thereof.
2. Where a decision adopted in accordance with Chapter 2 of Title V of the Treaty on European Union so provides, the Council may adopt restrictive measures under the procedure referred to in paragraph 1 against natural or legal persons and groups or non-State entities.
3. The acts referred to in this Article shall include necessary provisions on legal safeguards.

The complete consolidated version of the TFEU can be found on: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012E/TXT

TEEC: Treaty Establishing the European Economic Community. See TEC.

Terrorist: According to the FATF Recommendations Glossary, the term refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts ; (iii) organises or directs others to commit terrorist acts ; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

Terrorist Financing: According to the FATF Recommendations Glossary: The financing of terrorist acts, and of terrorists and terrorist organisations.

Testimony: A witness's oral presentation, usually under oath, of facts about which he or she has knowledge.

TFEU: Treaty on the Functioning of the European Union. See TEC.

Trade sanctions: These sanctions are applied for purely economic reasons, and typically take the form of tariffs or similar measures, rather than bans on trade. Trade sanctions are the most common kind and are the least onerous. They could be revocation of preferential treatment such as Most Favored Nation status or import quotas against a country not abiding by agreed international rules of trade.

Transaction screening: The process of screening a movement of value within the financial institution's records, including funds, goods or assets, between parties and accounts. In order to mitigate risk associated with trade finance transactions and international wire transfers, financial institutions conduct real-time screening of cross-border transactions against Sanctions Lists, where any of the sending bank, originating bank, receiving bank, intermediary bank or beneficiary bank are located in different countries. This definition is provided in the Wolfsberg Screening Guidance.

Travel ban: consist of restrictions or prohibitions on travel by designated individuals.

TWEA: Trading With the Enemy Act. One of the U.S. federal statutes that contains the substantive offences leading to or supporting a sanction under OFAC (Office of Foreign Assets Control).

U

UN: United Nations. The United Nations was established on October 24, 1945, by 51 countries committed to preserving peace through international cooperation and collective security. Today, nearly every nation in the world belongs to the UN. The United Nations Security Council issues a Consolidated UN Security Council Sanctions List. See www.un.org.

UN Consolidated Sanctions List: This list includes all individuals and entities subject to sanctions measures imposed by the UN Security Council. The inclusion of all names on one Consolidated Sanctions List is to facilitate the implementation of the measures, and neither implies that all names are listed under one regime, nor that the criteria for listing specific names are the same. For each instance where the Security Council has decided to impose sanctions in response to a threat, a Security Council Committee manages the sanctions regime. Each sanctions committee established by the United Nations Security Council publishes the names of individuals and entities listed in relation to that committee as well as information concerning the specific measures that apply to each listed name. The Consolidated Sanctions List is provided in .xml, .html and .pdf formats. Member States are obliged to implement the measures specific to each listed name as specified on the websites of the related sanctions committee. See: https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

United Nations Security Council Resolution: Security Council resolutions bind U.N. member states, unlike treaties or conventions that require subsequent steps by the signatory nations.

United Nations Security Council: The UN Security Council can take action to maintain or restore international peace and security under Chapter VII of the United Nations Charter. Sanctions measures, under Article 41, encompass a broad range of enforcement options that do not involve the use of armed force. Sanctions resolutions must pass the fifteen-member Council by a majority vote and without a veto from any of the five permanent members: the United States, China, France, Russia, the UK. Since 1966, the Security Council has established 26 sanctions regimes, in Southern Rhodesia, South Africa, the former Yugoslavia, Haiti, Iraq, Angola, Sierra Leone, Somalia, Eritrea, Liberia, DRC, Côte d'Ivoire, Sudan (2), Lebanon, DPRK, Iran, Libya (2), Guinea-Bissau, CAR, Yemen and South Sudan, as well as against Al-Qaida and the Taliban (2). Security Council sanctions have taken a number of different forms, in pursuit of a variety of goals. The measures have ranged from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and financial or commodity restrictions. The Security Council has applied sanctions to support peaceful transitions, deter non-constitutional changes, constrain terrorism, protect human rights and promote non-proliferation. Sanctions do not operate, succeed or fail in a vacuum. The measures are most effective at maintaining or restoring international peace and security when applied as part of a comprehensive strategy encompassing peacekeeping, peacebuilding and peacemaking. Contrary to the assumption that sanctions are punitive, many regimes are designed to support governments and regions working towards peaceful transition. The Libyan, Liberian and Guinea Bissau sanctions regimes all exemplify this approach. There are several UN ongoing sanctions regimes which focus on supporting political settlement of conflicts, nuclear non-proliferation, and counter-terrorism. Regimes are administered by a UN sanctions committee chaired by a non-permanent member of the Security Council. There are also monitoring groups, teams and panels of experts that support the work of the sanctions committees.

United Nations Security Council Sanctions Committees: The UNSC has several subsidiary organs, including sanctions committees. The Committees carry out the actual work with respect to a sanctions program. Their role is to implement, monitor and provide recommendations to the Council on particular sanctions regimes. A committee may request advice and meet with various Panels of Experts. The committee may also meet with Member States and international organizations. One important function of a committee is to identify exactly who is subject to sanctions. In some cases, the resolution creating a sanctions program may identify individuals or groups that will be subject to the sanctions, but in many cases, it is the responsible committee that does so. See: https://www.un.org/sc/suborg/en/scsb

Unilateral Sanctions: Sanctions imposed by a single country, such as the U.S. sanctions against Cuba.

UNSCR 1267: This UN Security Council Resolution created a regime that targets individuals and entities associated with Al Qaida requiring states to freeze the assets of persons designated under that regime. Countries implement these resolutions either directly in their national laws, or in the EU, after the EU issues a regulation. For example, the UK implements UN asset freezes by way of EU Regulation which takes direct effect in the UK. According to the UK National Risk Assessment of Money Laundering and Terrorist Financing of October 2015, it takes three to four weeks on average for the EU to implement UN listings resulting in a delay between the adoption of designations at the UN and their implementation and a possible risk of asset flight.

UNSCR 1373: On September 28, 2001, the U.N. Security Council unanimously adopted UNSCR 1373, which requires, among other things, the freezing of terrorist assets. The Security Council's action, in placing Resolution 1373 under Chapter VII of the U.N. Charter, signifies the urgency of its response. That chapter empowers the Security Council to enforce the terms of a resolution by use of measures ranging from economic sanctions to the use of military force on non-complying nations. UNSCR 1373 requires states to freeze the assets of terrorists and prohibit their nationals and persons within their jurisdiction from making funds, resources or financial services available to them.

USA PATRIOT Act: An acronym for the Uniting and Strengthening America by Providing Appropriate Tools needed to Intercept and Obstruct Terrorism Act of 2001. Made up of 10 Titles, the Act (Public Law 107-56) became law on October 26, 2001, only 45 days after the September 11 2001 terrorist attacks. This historic law brought about momentous changes, including more than 50 amendments to the Bank Secrecy Act. Title III of the Act, the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, contains most, but not all, of the money laundering-related provisions of the Act. Titles II and IV extend the powers of U.S. law enforcement agencies, as well as extend the sharing of information between various law enforcement, prosecutorial, and intelligence agencies. Section 221 of the Act which is titled, "Trade Sanctions" is included in Title II of the Act, named "Enhanced Surveillance Procedures."

U.S. Department of State Office of Economic Sanctions Policy and Implementation: (EB/TFS/SPI) is responsible for developing and implementing foreign policy-related sanctions adopted to counter threats to national security posed by particular activities and countries. SPI builds international support for implementation of economic sanctions, provides foreign policy guidance to the Department of Treasury and Commerce on sanctions implementation, and works with Congress to draft legislation that advances U.S. foreign policy goals in these areas. SPI maintains and enforces sanctions to maximize their economic impact on our targets and minimize the damage to U.S. economic interests. We also work to remove economic sanctions when appropriate to reward and incentivize improved behavior or demonstrate U.S. support for newly established democratic governments. In addition, SPI conducts outreach on sanctions issues to a wide range of interested parties including NGOs, companies, diaspora groups, and others. https://www.state.gov/economic-sanctions-programs/

V

…

W

Wassenaar Arrangement: This is the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. The name comes from Wassenaar, a town located in a suburb of the Hague, Netherlands, where an agreement was reached in 1995 to start a new type of multilateral co-operation. The Wassenaar Arrangement has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. Participating States seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists. Representatives of Participating States meet regularly in Vienna where the Wassenaar Arrangement has established its headquarters and a small Secretariat. See: http://www.wassenaar.org

Warrant: A written order or writ from a competent authority directing the doing of a certain act.

Watchlist: A list prepared internally by organizations identifying individuals or entities whose activities are to be monitored closely.

Weak AKA: A “weak AKA” is a term used by OFAC and Wolfsberg 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. 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. OFAC has instituted procedures that attempt to make this qualitative review of aliases as objective as possible. In the TXT and PDF versions of the SDN List, weak AKAs are encapsulated in double-quotes within the AKA listing: For example: 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). See: https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/weak_strong_alias.aspx. OFAC's regulations do not explicitly require any specific screening regime. Financial institutions and others must make screening choices based on their circumstances and compliance approach. As a general matter, though, OFAC does not expect that persons will screen for weak AKAs, but expects that such AKAs may be used to help determine whether a "hit" arising from other information is accurate.

White-Collar Crime: A type of crime generally seen as non-violent or involving more sophisticated, "business-related" schemes rather than crimes of violence or street crime. Such crimes include tax fraud (evasion, false tax returns, failure to file tax returns), money laundering (any attempt to hide money derived from illegal sources), bribery, bankruptcy fraud, environmental fraud, health care fraud and many others.

Willful Blindness: A legal principle that operates in money laundering, forfeiture and other cases in the United States, the United Kingdom and other countries. It has been defined by courts as the "deliberate avoidance of knowledge of the facts" or "purposeful indifference." Courts have held in several money laundering cases that willful blindness is the equivalent of actual knowledge of the illegal source of funds or of the intentions of a customer in a money laundering transaction.

Wire Transfers: The electronic transmission of funds between financial institutions on behalf of themselves or their customers. Wire transfers are financial vehicles covered by the statutory or regulatory requirements of many countries as part of their anti-money laundering and anti-terrorist financing effort. Also known as EFTs, or Electronic Funds Transfers.

Without Delay: According to the FATF Recommendations, this phrase means, ideally, within a matter of hours of a designation by the United Nations Security Council or its relevant Sanctions Committee (e.g. the 1267 Committee, the 1988 Committee, the 1718 Sanctions Committee or the 1737 Sanctions Committee). For the purposes of S/RES/1373(2001), the phrase without delay means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organisation. In both cases, the phrase without delay should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to terrorists, terrorist organisations, those who finance terrorism, and to the financing of proliferation of weapons of mass destruction, and the need for global, concerted action to interdict and disrupt their flow swiftly.

Wolfsberg Group: The Wolfsberg Group consists of leading international financial institutions. Wolfsberg has issued Wolfsberg AML Princples, and other documents, and is named after the city in Switzerland where the first working session of the group to formulate the guidelines was held.

Wolfsberg Guidance on Sanction Screening: Paper issued by the Wolfsberg Group in 2019 providing guidance to financial institutions as they assess the effectiveness of their sanctions screening controls, whether automated, manual or both.

https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf

World Bank Debarred List: A list issued by the World Bank containing those sanctioned under the World Bank's fraud and corruption program. See:

http://web.worldbank.org/external/default/main?theSitePK=84266&contentMDK=64069844&menuPK=116730&pagePK=64148989&piPK=64148984

X

…

Y

…

Z

…

PRACTICE QUESTIONS

Practice Questions for the CSS Examination

1. **Which of the following is *not* an objective of economic sanctions?**

    a. To deny resources to targets of sanctions

    b. To send a political message

    c. To provide the sanctioning country's industries with a competitive advantage

2. **The United Nations imposes sanctions**

    a. Against individuals, entities, and countries

    b. Against individuals and entities only

    c. Against countries only

3. **Under the EU sanctions regime, sanctions are imposed by**

    a. The EU Commission

    b. The EU Council

    c. The EU Parliament

4. **Sanctions that the United States may impose against non-U.S. parties for failure to comply with U.S. sanctions are called**

    a. Secondary sanctions

    b. Direct sanctions

    c. Sectoral sanctions

5. **Under the U.S. system, designation as an SDN also applies automatically to**

    a. Entities owned or controlled by SDNs

    b. Entities owned 50 percent or more by any combination of SDNs

    c. Owned 50% or more by a single SDN

6. Which of the following is a red flag for a financial transaction?

a. The payment crosses international boundaries

b. The payment is denominated in a currency different from that of the countries of the parties involved

c. Key information in a payment message has been omitted

7. Which do both OFAC and the EU identify as the first key element to a sanctions compliance framework and compliance program for dual-use trade controls, respectively?

a. Management commitment to compliance

b. A system for screening customers and transactions

c. A written sanctions policy

8. "Screening" refers to

a. An automated system for identifying key words in data fields

b. Any sort of review of information regarding a person or transaction to determine if sanctioned elements are present

c. A process for assessing the sanctions risk of a transaction

9. A specific license is valid with respect to

a. All parties identified in the license

b. The applicant for the license only

c. All parties performing the sorts of transactions identified in the license

10. A filing with a legal authority regarding potential sanctions violations is known as

a. A retroactive license application

b. A notice of possible violation

c. A voluntary self-disclosure

Answers:

1. C
2. A
3. B
4. A
5. B
6. C
7. A
8. B
9. A
10. C

ASSOCIATION OF CERTIFIED SANCTIONS SPECIALISTS

Association of Certified Sanctions Specialists (ACSS)
7950 NW 53rd Street Suite 337
Miami, FL 33166
Phone: +1 305 433 7187
helpdesk@sanctionsassociation.org
www.sanctionsassociation.org