Annual Survey of U.S. Economic Sanctions and Export Controls

Michael T. Gershberg

International Corporate Compliance Executive Seminar

April 26, 2023

Copyright © 2023 Fried, Frank, Harris, Shriver & Jacobson LLP. All rights reserved.

Fried Frank

Agenda

Economic Sanctions

- Policy and Legal Overview
- Recent Developments
- Enforcement Case Studies

Export Controls

- Policy and Legal Overview
- Recent Developments
- Enforcement Case Studies

Fried Frank

ECONOMIC SANCTIONS: POLICY AND LEGAL OVERVIEW

Fried Frank

U.S. Economic Sanctions

Advance U.S. national security and foreign policy objectives

- "Name and shame" function
- Deprive their targets of economic resources and access to global markets
- Isolate sanctions targets generally

U.S. economic sanctions are an instrument of statecraft

- Economic sanctions can be implemented quickly
- Complement other instruments of U.S. statecraft (*e.g.*, diplomacy, military power)
  - Sanctions have been issued prohibiting transactions with Crimea and sanctioning Russian companies and institutions in response to Russia's actions in Ukraine
  - The United States has relaxed, and then strengthened, Iran-related sanctions to advance its goal of halting Iranian nuclear weapons development
  - Additional sanctions have been imposed on Iran and North Korea in response to Iranian ballistic missile development and North Korean nuclear weapons development
  - Cuba sanctions have been adjusted in order to support the Cuban private sector and civil society

U.S. Economic Sanctions (Cont'd)

Jurisdiction

- U.S. Persons
  - U.S. citizens or permanent residents (Green Card holders), wherever located
  - Entities organized in the U.S. (including foreign branches owned and controlled by a U.S. entity)
  - Persons "within the territory" of the U.S.
- Non-U.S. companies owned or controlled by U.S. persons (Cuba and Iran programs only)

Impact

- Prohibit direct and indirect transactions (*e.g.*, export, financial, import, etc.) with and / or impose investment restrictions on sanctioned parties and countries

Practice Points

- Country-based sanctions *and* list-based sanctions
- Extent of country-based sanctions varies by program (*e.g.*, (comprehensive) Iran, Cuba, Crimea *vs.* (targeted) Libya, Zimbabwe, etc.)
- Hybrid targeted sanctions on Russia and Venezuela
- Prohibit "facilitation" (*e.g.*, U.S. persons assisting non-U.S. persons in activities that the former cannot do directly)

U.S. Sectoral Sanctions

- Sectoral sanctions are a less severe form of sanctions than traditional OFAC sanctions
- They seek to prohibit certain behavior relating to specific industrial sectors, rather than a comprehensive trade embargo or ban on dealing with certain persons
- Currently, sectoral sanctions only apply to Russia / Ukraine
- OFAC has created the Sectoral Sanctions Identifications List or "SSI List" identifying sanctioned parties under the sectoral sanctions
- Parties are added to the SSI List as subject to certain Directives
    - Directives 1-3 prohibit dealing in new debt (and in some cases new equity) that exceeds 14, 30, or 60 day maturity periods, of persons listed on the SSI list under those Directives
        - Directive 1 contains persons in the Russian financial services sector
        - Directive 2 contains persons in the Russian energy sector
        - Directive 3 contains persons in the Russian defense and materials sector
    - Directive 4 prohibits activities in support of exploration or production for frontier oil projects in Russia related to persons in the Russian energy sector, or globally if owned by such persons

Penalty Framework

	Civil Penalties	Criminal Penalties
International Emergency Economic Powers Act (IEEPA)	$356,579 per violation or twice the amount of the underlying transaction, whichever is greater	$1,000,000 and up to 20 years imprisonment
Trading with the Enemy Act (TWEA)	$105,083 per violation	$1,000,000 fine for corporations; $100,000 for individuals; Forfeiture of funds or other property involved in violations; Up to 10 years imprisonment
Foreign Narcotics Kingpin Designation Act (Kingpin Act)	$1,771,754 per violation	$5,000,000 and up to 30 years imprisonment

Penalty Calculations

Pre-penalty notice – OFAC will issue a pre-penalty notice setting out a proposed penalty amount in accordance with the below matrix

BASE PENALTY MATRIX

Voluntary Self-Disclosure	Egregious Case: NO	Egregious Case: YES
YES	(1) One-Half of Transaction Value (capped at lesser of $178,290 or one-half of the applicable statutory maximum per violation)	(3) One-Half of Applicable Statutory Maximum
NO	(2) Applicable Schedule Amount (capped at lesser of $356,579 or the applicable statutory maximum per violation)	(4) Applicable Statutory Maximum

"General Factors" in Determining Penalty

- General Factors
  - A) Willful or reckless violation of law
    - This factor considers, willfulness, recklessness, concealment, pattern of conduct, prior notice and management involvement
  - B) Awareness of conduct at issue
    - This factor considers whether there was actual knowledge or reason to know, and management involvement
  - C) Harm to sanctions program objectives
    - This factor considers whether there was an economic or other benefit to a sanctioned person or country, implications for U.S. policy, license eligibility, and whether the activity was in support of humanitarian activity
  - D) Individual characteristics
    - This factor considers the commercial sophistication, size of operations, and sanctions history of the violator and the volume of the transactions
  - E) Compliance program
    - This factor considers the existence, nature, and adequacy of the violator's risk-based compliance program
  - F) Remedial response
    - This factor considers the nature and adequacy of any remedial measures taken by the violator
  - G) Cooperation with OFAC
    - This factor considers the nature and extent of cooperation with OFAC and whether the violation was voluntarily disclosed
- Egregiousness determination
  - OFAC determines if a case is egregious based on an analysis of General Factors A, B, and F, with particular emphasis on General Factors A and B

Fried Frank

Mitigation Considerations

- Voluntary self-disclosure of alleged violations
- Cooperation with OFAC
- Establishing and maintaining a “risk-based” compliance policy
- Multiple violations caused by substantially similar acts
- Agreeing to conduct a meaningful compliance review
- Taking remedial measures
- Absence of prior OFAC penalties in the recent past

U.S. Economic Sanctions — Extraterritoriality

- Long history of application of sanctions **against non-U.S. persons** for conduct outside the U.S.
  - 1960s—Fruehauf France
  - 1980s—Siberian Pipeline Sanctions; Toshiba Sanctions
  - 1990s—Helms-Burton Act; Iran and Libya Sanctions Act
  - 2000s—Sudan Accountability and Divestment Act
  - 2010s—
    - Comprehensive Iran Sanctions, Accountability and Divestment Act (CISADA)
    - Iran Threat Reduction and Syria Human Rights Act of 2012 (ITRSHRA)
    - Iran Freedom and Counter-Proliferation Act of 2012 (IFCA)
    - Ukraine Freedom Support Act (2014)
    - North Korea Sanctions and Policy Enhancement Act of 2016
    - Countering America's Adversaries Through Sanctions Act (CAATSA) (2017)
    - Hong Kong Autonomy Act (2020)

ECONOMIC SANCTIONS: RECENT DEVELOPMENTS

Fried Frank

Economic Sanctions – Overview

- Russia / Ukraine Sanctions
- New Sanctions Programs and Authority
- Chinese Military Sanctions
- Iran Sanctions Following JCPOA Withdrawal in 2018
- Venezuela Sanctions
- Cuba Sanctions
- Changes to Reporting Regulations
- Sanctions Compliance Framework
- Policy and Regulatory Trends

Fried Frank

Russia / Ukraine-Related Sanctions

- Throughout 2019, 2020, and 2021, OFAC issued a number of new sanctions on Russia in response to the imprisonment of Alexei Navalny, malicious cyber activities, and foreign election interference
  - In September 2019, OFAC issued a directive prohibiting U.S. financial markets from participating in the primary market for non-ruble denominated bonds issued by the Russian Government
  - In March 2021, OFAC designated the Russian Federal Security Service ("FSB") as a blocked party under the Weapons of Mass Destruction Sanctions Regulations
    - OFAC issued a general license to permit U.S. persons to interact with the FSB for purposes of qualifying their products for importation and distribution in Russia
    - This designation created an SEC reporting obligation under the Iran Threat Reduction Act, which requires issuers to disclose if they or their affiliates knowingly conducted dealings with persons subject to OFAC WMD or Anti-Terrorism sanctions
    - The general license does not eliminate the disclosure requirement under 13(r)
- **Sovereign debt sanctions:**
  - In April 2021, President Biden issued Executive Order 14024, which authorized new sanctions on Russia. OFAC simultaneously issued Directive 1, which prohibits U.S. financial institutions from participating in the primary market for ruble or non-ruble dominated bonds issued by the Russian Central Bank, the National Wealth Fund, or the Russian Ministry of Finance

Russia / Ukraine-Related Sanctions (Cont'd)

- **Donetsk People's Republic ("DNR") and Luhansk People's Republic ("LNR") sanctions:**
- On February 21, 2022, in response to Russia recognizing the so-called Donetsk and Luhansk People's Republics, President Biden issued Executive Order 14065, which imposes comprehensive sanctions on the two regions. E.O. 14065 tracks similar comprehensive sanctions on Crimea, and prohibits:

  (1) new investment in the DNR or LNR

  (2) the importation, directly or indirectly, of any goods, services, or technology from the DNR or LNR

  (3) the exportation, reexportation, sale, or supply from the United States or by a U.S. person of any goods, services, or technology to the DNR or LNR

- The E.O. further prohibits any approval, financing, facilitation, or guarantee by a U.S. person of a transaction by a foreign person that would be prohibited if the transaction were performed by a U.S. person or within the United States
- Concurrently with the publication of E.O. 14065, OFAC issued six general licenses allowing for wind down transactions, the export of agricultural commodities and medicine, transactions related to telecommunications, official business by international organizations, personal remittances, and transactions related to internet-based communications

Fried Frank

Russia / Ukraine-Related Sanctions (Cont'd)

- **Additional restrictions on dealing in Russian sovereign debt:** Directive 1A prohibits U.S. financial institutions from participating in the secondary market for ruble or non-ruble denominated debt issues by the Russian Central Bank, National Wealth Fund, or Ministry of Finance. Previously only primary market transactions were prohibited
- **Sanctions on correspondent and payable through accounts:** Directive 2 prohibits U.S. financial institutions from opening or maintaining correspondent or payable-through accounts for or on behalf of Sberbank or Sberbank subsidiaries
  - Directive 2 took effect on March 26, 2022
  - It prohibits U.S. financial institutions from processing transactions for Sberbank and its subsidiaries
  - U.S. financial institution means any U.S. entity, including foreign branches, that is engaged in the business of accepting deposits, making, granting, transferring, holding, or brokering loans or credits, or purchasing or selling foreign exchange, securities, or futures or options, or procuring purchasers and sellers thereof
    - This includes banks, money service businesses, operators of credit card systems, trust companies, insurance companies, securities brokers and dealers, options brokers and dealers, exchanges, clearing corporations, and investment companies

Russia / Ukraine-Related Sanctions (Cont'd)

- **Restrictions on dealing in new debt / equity:** Directive 3 prohibits the U.S. from dealing in new equity and new debt with a maturity of longer than 14 days issued by designated companies in the Russian financial and energy sectors after March 26, 2022. This directive applies to, among others:
  - Sberbank
  - Gazprombank, Gazprom, and Gazprom Neft
  - Alfa-Bank
  - Rostelecom, RusHydro, Alrosa, Sovcomflot, and Russian Railways
- **Central Bank of Russia sanctions:** Directive 4 prohibits any transaction involving the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, and the Ministry of Finance, including any transfer of assets to such entities or any foreign exchange transaction for or on behalf of such entities
- **General licenses** temporarily authorize certain wind-down activities and energy-related transactions
- **Blocking sanctions:**
  - OFAC imposed blocking sanctions against a number of Russian banks and their subsidiaries, including VEB, Promsvyazbank, VTB Bank, Otkritie, Sovcombank, and Novikombank
  - OFAC imposed blocking sanctions against the Russian Direct Investment Fund (RDIF), a Russian sovereign wealth fund, and its management company and CEO
- **SWIFT sanctions:** The EU, UK, and US agreed to remove a number of major Russian banks, including Sovcombank, VEB, and VTB from SWIFT. In May 2022, the EU also removed Sberbank from SWIFT

Fried Frank

Russia / Ukraine-Related Sanctions (Cont'd)

- **Ban on most energy product imports** – Executive Order 14066, issued on March 8, 2022 bans the importation into the United States of Russian-origin crude oil, petroleum, petroleum fuels, oil, liquefied natural gas, coal, and coal products. oil, petroleum, petroleum fuels, oil, liquefied natural gas, coal, and coal products
- **Crude oil / petroleum products price cap**: In November 2022, the U.S., EU, Australia, and the G7 announced price caps for Russian-origin crude oil and petroleum products. These price caps operate by prohibiting the import of certain products unless they are below the agreed upon price cap
  - U.S. persons are prohibited from engaging in various services ("covered services") relating to Russia-origin oil and petroleum products unless it involves products purchased at or below the applicable price cap. The covered services include trading / commodities brokering, financing, shipping, insurance, reinsurance, flagging, and customs brokering
  - Price cap for crude oil: $60/barrel (effective December 5, 2022)
  - Price cap for Discount to crude petroleum products: $45/barrel (effective February 5, 2022)
    - This covers naphtha, residual fuel oil, and waste oils
  - Price cap for Premium to crude petroleum products: $100/barrel (effective February 5, 2022)
    - This covers gasoline, motor fuel blending stock, gasoil and diesel fuel, kerosene and kerosene-type jet fuel, and vacuum gas oil

Fried Frank

Russia / Ukraine-Related Sanctions (Cont'd)

- **Prohibition on new investment in the Russian Federation –** Executive Order 14071, issued in April 2022, prohibits "new investment" in Russia. Subsequently, OFAC has issued guidance and FAQs making clear that the new investment ban **is not** a comprehensive prohibition on dealings with Russia
- **FAQ #1049:** "Investment" means the commitment of capital or other assets for the purpose of generating returns or appreciation. New investment includes:
  - The purchase or acquisition of real estate in Russia;
  - The purchase or acquisition of rights to natural resources in Russia;
  - The formation of JVs or other corporate entities in Russia;
  - Entering an agreement providing for the participation in royalties or ongoing profits in Russia;
  - The lending of funds to persons located in the Russian Federation for commercial purposes; and
  - The purchase of an equity interest in an entity located in Russia
- **FAQ #1054**: U.S. persons are not prohibited from selling or divesting debt or equity securities issued by a Russian entity to a non-U.S. person
  - Additionally, U.S. financial institutions are not barred from clearing and settling, or otherwise serving as market intermediaries in, divestment transactions on the secondary market
- **FAQ #1055 –** U.S. persons may lend funds to or purchase debt and equity interests in entities located outside of Russia, provided that (i) such funds are not specifically intended for new projects or operations in the Russian Federation and (ii) the entity located outside Russia derives less than 50 percent of its revenues from its investments in Russia

Fried Frank

New Sanctions Programs – Belarus and HKAA

- **Belarus -** In August 2021, President Biden issued Executive Order 14038, which authorized sanctions on Belarus and imposed blocking sanctions on persons in Belarus's defense, security, energy, potash, tobacco, construction, and transportation sectors
  - December 2021: Directive 1 – Prohibits dealings in Belarusian sovereign debt with a maturity of greater than 90 days. Covers both primary and secondary markets for debt issued by the Ministry of Finance and the Development Bank of the Republic of Belarus
  - February 2022: OFAC made additional designations in response to Belarus's support for the Russian invasion of Ukraine, targeting persons in the defense and security sectors, as well as two state owned banks (Belinvestbank and Bank Dabrabyt)
- **Hong Kong Autonomy Act (HKAA)** – In June 2020, President Trump signed the HKAA into law, which provides for property- and visa-blocking sanctions on persons deemed to have materially contributed to China's crackdown in Hong Kong ("Material Contributors")
  - The Act also requires the Secretary of State to identify any foreign financial institutions that knowingly conduct a significant transaction with a Material Contributor
  - OFAC has clarified that U.S. persons can engage in dealings with Hong Kong government agencies in which a SDN is an official as long as the interactions do not directly or indirectly involve the SDN

Fried Frank

New Sanctions Programs – Burma

- On February 10, 2021, President Biden issued Executive Order 14014, which authorized OFAC to sanction individuals determined to be, among other things:
  - Operating in the defense sector of the Burmese economy,
  - Having been a leader or official of the government or military or security forces of Burma,
  - Being a subdivision, agency or instrumentality of the government of Burma,
  - Engaging or attempting to engage in actions that undermine democratic processes or institutions in Burma, threaten peace, security or stability of Burma, limit free expression, or constitute serious human rights abuses, or
  - Providing material support for any person sanctioned under the E.O.
- On June 1, 2021, OFAC issued the Burma Sanctions Regulations, which provide a framework similar to other US list-based sanctions regimes
- In February 2022, the U.S. designated additional Burmese persons in the defense sector and associated with the Burmese military

New Sanctions Programs – Ethiopia

- On September 17, 2021, President Biden issued Executive Order 14046, authorizing OFAC to implement targeted sanctions in response to the conflict in Ethiopia's Tigray region. The EO provides for the designation of any person who is determined to be responsible for, complicit in, or to have engaged in a range of activities related to the conflict
- The EO allows OFAC to utilize menu-based sanctions and take the following actions:
  - Block all property and interests in property of the sanctioned person (i.e., designation on the SDN List);
  - Prohibit any U.S. person from investing in or purchasing significant equity or debt of the sanctioned person;
  - Prohibit any U.S. financial institution from making loans or providing credit to the sanctioned person;
  - Prohibit any transactions in foreign exchanges that are subject to U.S. jurisdiction in which the sanctioned person has any interest; or
  - Impose any of the above sanctions on the principal executive officers of any sanctioned entity
- OFAC's 50 Percent Rule does not automatically apply to persons blocked pursuant to EO 14046. A subsidiary designated pursuant to the EO 14046 is not considered blocked unless it is itself a sanctioned person listed separately on the SDN List or on the Non-SDN Menu-Based Sanctions List
- OFAC has issued three general licenses authorizing, generally, activities for the conduct of official business of the UN, Red Cross, African Union, and other specified international organizations, transactions related to certain activities of NGOs, and transactions ordinarily incident to the export or reexport of agricultural commodities, medicine, and medical devices

Chinese Military Companies Sanctions

- On November 12, 2020, President Trump issued Executive Order 13959, which prohibited U.S. persons from trading securities and related derivatives of companies designated as Communist Chinese Military Companies ("CCMCs")
- On June 3, 2021, President Biden issued Executive Order 14032, which revised and superseded E.O. 13959. This new E.O. placed similar investment restrictions on Chinese Military-Industrial Companies ("CMICs"). Most of the designated companies operate in the Chinese defense sector, although some (Hikvision and Huawei) were designated for operating in the Chinese surveillance sector
- **CMIC sanctions overview:**
  - U.S. persons are prohibited from investing or otherwise transacting in publicly traded securities of designated CMIC companies and any "securities that are derivative of or are designed to provide investment exposure to such securities"
    - This includes warrants, American depositary receipts (ADRs), global depositary receipts (GDRs), exchange-traded funds (ETFs), index funds, and mutual funds
  - U.S. persons may still provide advisory, investment management, or similar services to a non-U.S. person in connection with the non-U.S. person's purchase or sale of a security covered by CMIC sanctions, provided that the underlying transaction would not otherwise violate the CMIC sanctions
  - There is a one-year wind-down period in which market makers may participate in activities necessary to effect the divestiture of covered securities currently held by the U.S.
  - The prohibitions of E.O. 14032 do not apply to a subsidiary of a CMIC unless that subsidiary is itself designated by OFAC

Fried Frank

Iran Sanctions – Withdrawal From the JCPOA

- On **May 8, 2018**, President Trump announced that the United States would withdraw from the Joint Comprehensive Plan of Action (JCPOA)
- All U.S. sanctions waived or relaxed pursuant to the JCPOA have been reimposed
- All Iranian persons and entities that were removed from the Specially Designated Nationals and Blocked Persons list (SDNs) have been re-added
- General License H has been revoked and non-U.S. subsidiaries of U.S. businesses may no longer do any business with Iran
- Imports to the U.S. of certain Iranian goods which were permitted by the JCPOA are now once again prohibited
- The European parties to the JCPOA have stated they remain committed to upholding the JCPOA
- The EU has extended its blocking statute to cover compliance with U.S. sanctions on Iran
- Since reimposing sanctions in 2018, the US has continued to add Iranian entities and individuals to the SDN List and has imposed new secondary sanctions on various sectors of the Iranian economy including construction, mining, manufacturing, and textiles

Expansion of Iran Sanctions

- On August 6, 2018, President Trump issued an executive order providing for expanded sanctions against Iran beginning November 5, 2018, coinciding with the full snap-back of Iran-related sanctions waived under the JCPOA
- The executive order expands Iran sanctions by:
  - Providing the authority for blocking sanctions against persons who have provided material support for certain blocked persons on or after November 5, 2018;
  - Providing the authority for correspondent and payable-through account sanctions on foreign financial institutions who conduct significant financial transactions for such persons on or after November 5, 2018;
  - Expanding the menu of sanctions available to impose on persons who engage in certain significant transactions relating to the Iranian petroleum or petrochemical industries on or after November 5, 2018 to include the following: (a) visa restrictions on officers and shareholders; (b) sanctions against officers and shareholders; and (c) prohibitions on U.S. investment or purchasing debt or equity; and
  - Expanding the scope of sanctions on U.S. owned or controlled foreign entities to prohibit transacting business with persons blocked for providing material support to Iranian Specially Designated Nationals (SDNs) or who are part of certain Iranian industries

Additional Iran Sanctions in 2019

- On May 8, 2019, President Trump issued an Executive Order imposing sanctions on Iran's iron, steel, aluminum, and copper sectors
    - The EO authorizes blocking sanctions on any person operating, engaging in significant transactions with, or providing material support to, any person in those sectors
    - The U.S. government may also place correspondent and payable-through account sanctions on foreign financial institutions that knowingly conduct or facilitate transactions related to those sectors, or related to any person blocked pursuant to the EO
- On June 24, 2019, President Trump issued an Executive Order imposing sanctions on Iran's Supreme Leader and other Iranian government officials
    - OFAC is authorized to designate other Iranian government officials not already sanctioned in the EO, and anyone who provides material support to the Supreme Leader's office as blocked persons
    - The EO also authorizes sanctions against foreign financial institutions that knowingly conduct or facilitate a significant transaction related to the designated persons

Additional Iran Sanctions in 2020 and 2021

- January 14, 2020, President Trump issued Executive Order 13902, which imposed new secondary sanctions on the construction, mining, manufacturing, and textile sectors of the Iranian economy
  - The EO authorizes blocking sanctions on any person operating, engaging in significant transactions with, or providing material support to, any person in these sectors
  - The EO also authorizes blocking sanctions on foreign financial institutions that conducted or facilitated financial transactions related to the above sectors
- September 21, 2020 – President Trump Issued EO 13949, which imposed additional sanctions on Iranian persons responsible for the proliferation of conventional arms
- October 8, 2020 – OFAC sanctioned 18 major Iranian financial institutions pursuant to Executive Order 13902

Syria Sanctions

- While comprehensive sanctions on Syria remain in place, OFAC has issued certain general licenses:
    - In May 2022, OFAC issued General License 22, which authorizes activities in a wide range of sectors (agriculture, information and telecommunications, power grid infrastructure, construction, finance, clean energy, transportation and warehousing, water and waste management, health services, education, manufacturing, and trade) in four non-government controlled regions in the north of Syria
    - In February 2023, OFAC issued General License 22, authorizing transactions related to earthquake relief
- Previously in 2020, OFAC designated additional members of the Syrian government, including the head of the Syrian General Intelligence Directorate, the Governor of the Central Bank of Syria, members of the Syrian parliament and Syrian military officials. OFAC also designated companies based in Syria and Lebanon that operate in Syria's petroleum industry

Venezuela Sanctions

- Beginning August 2017, the Trump administration has imposed major sanctions against Venezuela
- The sanctions aim to isolate Venezuela and its government from the U.S. financial system, to prevent U.S. person involvement in Venezuelan regime's raising capital at the expense of its citizens, and punish the Venezuelan government's expropriation of the country's assets
- Restrictions on dealing in new debt or new equity of Venezuela's government or state-owned enterprises, including PdVSA – similar to Russia's SSI sanctions
- Dealing in Venezuelan governmental bonds, securities, dividend payments, or cryptocurrency is prohibited
- A second round of sanctions was imposed in May 2018 aimed at preventing the government from collateralizing or selling state-owned assets
- Following these sanctions, U.S. persons are prohibited from transactions relating to:
  - purchasing debt of the Government of Venezuela;
  - debt owed to the Government of Venezuela that is pledged as collateral; and
  - the sale or pledging of collateral by the Government of Venezuela of any equity interest in which it owns 50% or more
- Under OFAC's 50% Rule, these sanctions apply to many joint ventures with PdVSA and the Government of Venezuela

Venezuela Sanctions (Cont'd)

- In November 2018, an Executive Order authorized sanctions against those operating in Venezuela's gold industry, in other sectors that OFAC may designate, and in programs involving the Government of Venezuela
  - The authority for OFAC to designate additional sectors is a potentially powerful tool
- In August 2019, President Trump issued a sweeping executive order freezing the property and assets of the Government of Venezuela, including state-owned companies
  - Various general licenses still authorize dealings with the Guaidó regime and transactions related to PdVSA and Citgo
  - U.S. persons may still deal with private Venezuelan entities and individuals
- OFAC designated the Central Bank of Venezuela as an SDN
- OFAC has sanctioned foreign shipping companies, including two subsidiaries of Rosneft, for transporting Venezuelan oil
- In June 2021, the Biden administration indicated that the U.S. will continue to impose sanctions barring a major shift in policy by the Maduro administration in Venezuela
- In November 2022, OFAC issued a general license permitting Chevron to pump and sell oil from its Venezuelan wells owned through a JV with PdVSA. A similar general license has been considered for ConocoPhillips

Fried Frank

Current Cuba-related Authorizations

- From 2014 through 2016, the Obama administration relaxed certain sanctions against Cuba and expanded the scope of authorized U.S. transactions with Cuba and Cuban entities
  - While tourist travel to Cuba is still prohibited, certain OFAC general licenses authorize travel to Cuba, including for governmental organizations, journalistic activity, professional research and meetings, humanitarian projects, certain export transactions, and activities of private foundations or institutes
  - Other authorizations cover telecommunications services, financial services, transactions with Cuban nationals in third countries, and the export of U.S.-origin goods to Cuba for authorized activities
- The Trump administration rolled back some of these authorizations, as announced in June 2017 and throughout 2019
- In April 2019, the U.S. Secretary of State announced that U.S. citizens could file lawsuits against foreign companies that use property seized by the Cuban government, overturning a long-standing policy to suspend Title III of the Helms-Burton Act of 1996

Current Cuba-related Authorizations (Cont'd)

- Sept 2020 – New CACR restrictions
  - Prohibiting any person subject to U.S. jurisdiction from lodging, paying for lodging, or making any reservation for or on behalf of a third-party to lodge at any property identified by the State Department as being owned or controlled by the Government of Cuba or member of the Cuban Communist Party
  - Prohibiting the importation into the U.S. of Cuban-origin alcohol and tobacco products, which was previously allowed under certain circumstances by several general authorizations
  - Eliminated the general authorization for athletic and non-athletic competitions and exhibitions, as well as the general license for attending professional meetings (specific licenses may still be obtained)
- In October 2020, OFAC amended the CACR to prohibit the processing of remittances through any entities on the Cuba Restricted List, which included the military-run Fincimex and GAESA
- However, the CACR authorize the provision of services related to the exchange of communications over the internet and services related to the exportation of communications-related items
  - These authorizations cover the provision of certain fee-based internet communications services such as e-mail or other messaging platforms, social networking, VOIP, web hosting, and domain-name registration. The authorizations also cover services related to many kinds of software (including applications) used on personal computers, cell phones, and other personal communications devices
- In January 2021, the State Department redesignated Cuba as a state sponsor of terrorism
- In June 2022, OFAC amended the CACR to lift the $1,000 quarterly limit on close relative remittances, permit donative remittances, and authorize travel and other transactions related to attending or organizing professional meetings or conferences in Cuba

Fried Frank

Changes to Reporting Regulations

- The Reporting, Procedures, and Penalties Regulations (RPPR) govern reporting of potentially problematic transactions to OFAC
- The RPPR were amended via interim final rule in June 2019
- Previously, only U.S. financial institutions were required to report rejected funds transfers
- The updated RPPR now covers all U.S. persons and persons subject to U.S. jurisdiction, not only U.S. financial institutions
  - The updated RPPR also extended recordkeeping requirements to all U.S. persons and persons subject to U.S. jurisdiction who engage in transactions subject to sanctions regulations
- This expanded universe of persons must now report all rejected transactions, including those for goods and services, and not just rejected funds transfers
- A far greater number of companies may now be required to submit reports to OFAC and keep records on rejected transactions

Fried Frank

Sanctions Compliance Framework

- On May 2, 2019, OFAC published *A Framework for OFAC Compliance Commitments*
- Though OFAC always stressed the importance of an OFAC compliance policy, it had never before published guidance as to what such a program looks like
- An ideal sanctions compliance program must incorporate at least five essential components:
  - Management Commitment
  - Risk Assessment
  - Internal Controls
  - Testing and Auditing
  - Training
- The guidance also indicates that an effective compliance program will be taken into account both when considering whether to mitigate a potential penalty under the Guidelines and determining whether a case is deemed "egregious"

Fried Frank

Policy and Regulatory Trends

- OFAC's main priorities include Iran, Russia, and China
- U.S. government has signaled a willingness to inflict financial pain on U.S. companies to achieve its international policy goals, especially with respect to Russia sanctions (but note a countervailing interest in imposing sectoral sanctions instead of SDN designations)
- U.S. government has returned to a historical trend of working to coordinate sanctions with the EU and UK (especially with respect to Russia), but also recognizes that there may be certain differing interests, particularly regarding Iran and Russia's energy sector
- Russia remains an area of uncertainty given the geopolitical situation, and the sanctions landscape continues to evolve as the situation on the ground develops
  - The U.S., EU, and UK continue to announce additional rounds of sanctions targeting different areas of Russia's economy
- For both Cuba-related and Iran-related sanctions, Congressional action is needed to end any comprehensive sanctions

Policy and Regulatory Trends (Cont'd)

- OFAC has increasingly focused on China for foreign policy reasons, and it appears likely for that trend to continue during the Biden administration
- OFAC has also emphasized targeting, including through SDN designations, virtual currency actors, primarily due to their role in facilitating sanctions violations and sanctions evasions
    - In April 2022, OFAC designated Hydra Market under EO 14024 for having operated in the financial services sector of the Russian economy
    - In May 2022, OFAC designated Blender.io, a virtual currency mixer. Tornado Cash, another virtual currency mixer was designated in August 2022 and, after a lawsuit challenging the designation, redesignated under E.O. 13964 and E.O 13722, for enabling malicious cyber activities that ultimately support North Korea's weapons of mass destruction program

Sanctions Enforcement

- In 2022, OFAC reported **16 penalties** / settlement agreements totaling approximately **$42.6 million.**
- In 2021, OFAC reported **20** penalties / settlement agreements totaling approximately **$20.9 million**
- In 2020, OFAC reported **16 penalties** / settlement agreements totaling approximately **$23.6 million**
- In 2019, OFAC reported **26 penalties** / settlement agreements totaling approximately **$1.289 billion**
- In 2018, OFAC reported **7 penalties** / settlement agreements totaling approximately **$71.5 million**
- In 2017, OFAC reported **16 penalties** / settlement agreements totaling approximately **$120 million**
- In 2016, OFAC reported **9 penalties** / settlement agreements totaling approximately **$21.6 million**

Fried Frank

Sanctions Case Studies

Microsoft Corporation (April 6, 2023)

- **$2,980,265 settlement** for violations of the Cuba, Iran, Syria, and Ukraine-/Russia-Related sanctions programs from 2012-2019; part of a joint enforcement effort with BIS ($624,013 for related violations of the EAR)
  - 1,339 violations that occurred in the context of Microsoft's volume licensing and sales programs, by which third-party Licensing Solution Partners (LSPs) negotiate commercial supply agreements with end customers and then bill those customers (with Microsoft Ireland billing the LSPs). Under these programs, Microsoft did not always obtain complete and accurate information on the end users, leading to 1,300+ sales to SDNs, blocked persons, and end customers in sanctioned jurisdictions
  - Microsoft's screening against restricted-party lists did not identify blocked parties not specifically listed on the SDN List, but owned 50 percent or more by SDNs, or SDNs' Cyrillic or Chinese names, even though many customers in Russia and China supplied order and customer information in their native scripts.
  - The process of facilitating Microsoft software downloads, license activations, product key verifications, and subsequent usages relied, at least in part, on U.S.-based servers and systems operated by employees in the U.S.
- **Aggravating factors**
  - The Microsoft entities demonstrated a reckless disregard for U.S. sanctions by failing to identify that more than $12,000,000 worth of software and services were exported from the United States through Microsoft systems and servers to SDNs, blocked persons, and to multiple sanctioned jurisdictions
  - Undermined foreign policy objectives
  - Microsoft is a world-leading technology company operating globally with substantial experience and expertise in software

Fried Frank

Sanctions Case Studies (Cont'd)

Microsoft Corporation (April 6, 2023)

- **Mitigating factors**
  - Persons in Microsoft's U.S. offices or management were not aware of the violations at the time and the apparent violations came to light through a self-initiated lookback and comprehensive investigation
  - The apparent violations were self-disclosed and Microsoft fully cooperated with OFAC's investigation
  - Microsoft terminated the accounts of all SDNs and blocker persons and deactivated the license keys to prevent such persons from accessing its software
  - Microsoft undertook significant remedial measures and enhanced its sanctions compliance program through substantial investment and structural change

Sanctions Case Studies (Cont'd)

Wells Fargo Bank, N.A. (March 30, 2023)

- **$30,000,000 settlement** for violations of the Iranian, Sudanese, & Syrian Sanctions Regulations between 2008 and 2015
  - Wells Fargo, and its predecessor Wachovia Bank provided a European bank with software that the bank used to process trade finance transactions with U.S.-sanctioned jurisdictions and persons. The software was customized in order to allow the foreign bank to handle international trade finance instruments, including those involving OFAC-sanctioned jurisdiction
  - Wachovia sought to eliminate the involvement of Wachovia personnel in non-OFAC-compliant transactions but the foreign bank's use of the software continued to rely on Wachovia's (and then Wells Fargo's) technology infrastructure at the bank's branch in Hong Kong and data facility in North Carolina
  - After Wells Fargo acquired Wachovia in 2008, Wells Fargo personnel raised on multiple occasions, including to senior management, the potential sanctions-related risks arising from the trade insourcing relationships it inherited from Wachovia
  - Wells Fargo facilitated 124 transactions processed by Bank A involving sanctioned parties or jurisdictions, totaling approximately $532,068,794, that would have been prohibited if performed by Wells Fargo or another U.S. person or within the United States
- **Aggravating factors**
  - The legacy business unit demonstrated reckless disregard for U.S. sanctions requirements when it specially designed and provided a software platform for the foreign bank to engage in transactions involving sanctioned jurisdictions or persons;
  - Senior management should reasonably have been aware that the foreign bank was using the software to engage in transactions with sanctioned jurisdictions and persons
  - Wells Fargo is (and Wachovia was) a large and commercially sophisticated international financial institution
- **Mitigating factors**
  - No penalty notice or Finding of Violation from OFAC in the five years before the violations began
  - The true magnitude of the sanctions harm from the conduct was more limited than the total value of the transactions conducted by the foreign bank and many of the apparent violations may have been eligible for general or specific licenses

Fried Frank

Sanctions Case Studies (Cont'd)

Bittrex, Inc. (October 11, 2022)

- **$24,280,829 settlement** for violations of multiple sanctions programs between 2014 and 2017
  - During the relevant time Bittrex operated 1,730 accounts that processed 116,421 virtual currency-related transactions totaling approximately $263 million in apparent violation of multiple sanctions program
  - Bittrex started offering its virtual currency services in March 2014, but it had no sanctions compliance program in place until December 2015, when it began verifying customer identity. It did not retain a third-party screening vendor until February 2016. Such screening was only against the SDN List until October 2017
  - Bittrex only begin restricting accounts and screening IP and other addresses associated with sanctioned locations after being issued a subpoena by OFAC in October 2017
- **Aggravating factors**
  - Bittrex failed to exercise due caution or care for its sanctions compliance obligations by operating without a sanctions compliance for nearly two years after it began offering virtual currency services
  - Bittrex had reason to know that some of its users were in sanctioned jurisdictions based on those users' IP addresses and physical address data
- **Mitigating factors**
  - No penalty notice or Finding of Violation from OFAC in the five years before the violations began
  - Bittrex was a small and new company at the time of most of the apparent violations
  - Bittrex provided substantial cooperation in connection with OFAC's investigation
  - Most of the transactions at issue were for a relatively small amount, and the volume of apparent violations represents a relatively small percentage of Bittrex's total annual transaction volume
  - Bittrex swift took a series of remedial measures

Fried Frank

Sanctions Case Studies (Cont'd)

Airbnb Payments, Inc. (January 3, 2022)

- **$91,179 settlement** for violations of the Cuban Assets Control Regulations between 2015 and 2020
  - Airbnb Payments conducted a review based on a sample of Airbnb "stays" and "experiences" and determined that it processed payments related to 3,464 stays for guests traveling for reasons outside of one of OFAC's 12 authorized categories
  - Airbnb Payments also processed payments for 3,076 experiences where Airbnb Payments failed to keep records in accordance with OFAC regulations
  - Airbnb launched in Cuba in 2015 following regulatory changes related to travel to Cuba and the scaling up of its services in Cuba appears to have outpaced the company's ability to manage the associated sanctions risks *via* its technology platform
  - These violations were discovered when Airbnb Payments launched a proactive review of its compliance and they were voluntarily reported to OFAC
- **Aggravating factors**
  - The violations undermined U.S. foreign policy towards Cuba at the time they occurred
  - Airbnb Payments is a large and sophisticated U.S.-based technology company
- **Mitigating factors**
  - No penalty notice or Finding of Violation from OFAC in the five years before the violations began
  - Airbnb Payments provided substantial cooperation in connection with OFAC's investigation by proactively reviewing compliance and reporting findings to OFAC
  - Airbnb Payments undertook significant remedial measures including IP blocking regime, required attestations for guests, and requiring hosts to certify that they are independent entrepreneurs

Fried Frank

Sanctions Case Studies (Cont'd)

Mashreqbank psc (November 9, 2021)

- **Finding of Violation** for violations of the Sudanese Sanctions Regulations **($100M penalty** was paid in a settlement with the NY Department of Financial Services)
  - Between January 2005 and February 2009, Mashreq's London branch processed 1,760 outgoing payments through financial institutions in the United States in violation of the SSR
  - Specifically, Mashreq London processed payments through U.S. financial institutions that related to U.S. dollar (USD) transfers from accounts of Sudanese banks held outside the United States
  - In the payment messages, Mashreq left the originating institution field blank and included the non-Sudanese beneficiary bank in the field for beneficiary bank. This made it impossible for Mashreq's U.S. correspondents to interdict the payments, leading to them being processed through the U.S. financial system
- Aggravating factors
  - Mashreq processed 1,760 transactions over several years in violation of the SSR, causing harm to the integrity of a U.S. sanctions program
  - Mashreq acted recklessly regarding its U.S. sanctions obligations when it employed payment practices that did not identify the involvement of U.S.-sanctioned parties in specific payments
  - Some senior-level Mashreq branch employees had actual knowledge of the conduct giving rise to the violations
- Mitigating factors
  - Mashreq provided substantial cooperation and voluntarily entered into a retroactive statute of limitations waiver agreement, without which OFAC would have been time-barred from charging any of the violations
  - No penalty notice or Finding of Violation from OFAC in the five years preceding the earliest violation
  - Significant compliance enhancements including, over $122M spent on new systems, consultants, additional compliance staff, training, and independent reviews

Fried Frank

Sanctions Case Studies (Cont'd)

Cameron International Corporation (September 27, 2021)

- **$1,423,766 settlement** for violations of the Ukraine-Related Sanctions Regulations
  - Cameron, a Texas-based supplier of goods and services for the oil and gas industry, provided services to Gazprom-Neft Shelf for an Artic offshore oil project
  - It provided these services when in July 2015 four U.S.-person senior managers at Cameron approved five contracts for its Romania subsidiary to supply goods to one of Gazprom-Neft Shelf's offshore oil exploration platforms located in the Russian Arctic
  - Gazprom-Neft Shelf is a wholly-owned subsidiary of Gazprom (identified on the SSI List) and was subject to Directive 4 restrictions
  - Cameron had a policy in place to comply with Directive 4, but the relevant compliance policies did not indicate that U.S.-person involvement in the activities of Cameron's foreign subsidiaries could violate Directive 4's prohibitions
  - In June 2017 Cameron submitted a notice of apparent violation following a compliance review after it was acquired by Schlumberger, a Dutch-organized company
- **Aggravating factors**
  - The U.S.-person senior managers were aware that their approvals were for contracts to supply goods to Gazprom-Neft Shelf for Arctic offshore oil production and exploration
  - Cameron provided a real economic benefit to Gazprom-Neft Shelf and acted directly contrary to US foreign policy objectives
  - Cameron is a large and commercially sophisticated firm with an extensive global presence and operates in an industry with significant sanctions risk
- **Mitigating factors**
  - Cameron took corrective action including identifying all employees who should recuse themselves from Russia-related activities and implementing an automatic block on all Russia-related orders to allow for additional review
  - Cameron cooperated with OFAC during the investigation

Fried Frank

Sanctions Case Studies (Cont'd)

Union de Banques Arabes et Francaises (January 4, 2021)

- **$8,572,500** settlement for violations of Syria-Related Sanctions Programs
  - Between August 2011 and April 2013, UBAF operated U.S. dollar accounts on behalf of sanctioned Syrian financial institutions and indirectly conducted USD business on behalf of these institutions through the U.S. financial system
  - Most violations involved UBAF's processing of internal transfers on behalf of Syrian entities that were followed by corresponding funds transfers through a U.S. bank. Other violations involved "back-to-back" letter of credit transactions
  - UBAF's actions during this time period demonstrated knowledge of OFAC sanctions laws, but it acted recklessly by failing to exercise a minimal degree of caution in accounting for the risks associated with providing USD-based services to sanctioned parties
- **Aggravating factors**
  - UBAF demonstrated a reckless disregard for its U.S. sanctions compliance obligations when it continued to provide USD services to sanctioned Syrian parties after the August 2011 expansion of U.S. sanctions on Syria
  - UBAF management had actual knowledge of the conduct giving rise to the violations
  - UBAF conferred significant economic benefit to sanctioned parties and caused significant harm to the integrity of U.S. sanctions
- **Mitigating factors**
  - UBAF had a compliance program in place at the time of the violations
  - UBAF voluntarily self-disclosed the violations to OFAC and cooperated with OFAC's investigation
  - UBAF invested substantial resources in improving its compliance program and undertook several remedial measures, including adopting a new Financial Security Charter, adopting new sanctions policies, providing training for all employees, and reviewing its business lines and terminating high risk business lines

Fried Frank

Economic Sanctions: Key Takeaways

- Three risk areas: ordinary course operations, corporate transactions, and allegations of wrongdoing
- With the expansion of U.S. sanctions in recent years, businesses will want to consider flexibility in contracts and a willingness to handle risk exposure
- OFAC has used enforcement announcements to provide compliance guidance, expectations
- U.S. economic sanctions can be violated by acts of "facilitation," which is interpreted broadly by OFAC and brings indirect activity with a sanctioned party within the regulatory purview of U.S. economic sanctions
- Comprehensive sanctions against Cuba and Iran remain and show no signs of weakening
- U.S. foreign policy may continue to broaden its reach by applying U.S. economic sanctions extraterritorially, especially in regard to China and Russia-related sanctions
- As political instability and tension continue to grow in certain regions of the world (*e.g.*, Iran, Syria, Ukraine, Venezuela), economic sanctions may be an increasingly favored tool for governments to foster desired political outcomes
- The Biden administration is likely to take a measured approach to altering sanctions programs that were expanded by President Trump

EXPORT CONTROLS: POLICY AND LEGAL OVERVIEW

Fried Frank

U.S. Export Controls Generally

Control worldwide transfer of U.S.-origin goods, software, and technology ("items"), as well as certain activities involving U.S. / non-U.S. persons

- Include non-U.S. items that come into U.S. commerce or which contain certain levels of U.S. content
- More than just physical hardware exports are controlled
  - Physical reexports and retransfers from one non-U.S. party to another
  - Technology transfers between U.S. and non-U.S. persons anywhere in the world (even inside the United States—so-called "deemed exports")
    - Covers transfer by any means, including email, Internet access, visual / oral disclosure

Protect U.S. national security and advance U.S. foreign policy

- Keep sensitive technology out of the wrong hands
- Preserve U.S. technological superiority and economic interests
- Promote regional stability, arms control, and compliance with international commitments

Some export-controlled activities require export license or other form of approval

- Defense trade strictly regulated—controlled activities require prior approval
- Most commercial exports and related activities do not require a license

Fried Frank

Bifurcated Export Control Regime

	Dual-Use Trade Controls	Defense Trade Controls
Law	Export Control Reform Act of 2018	Section 38 of the Arms Export Control Act, 22 USC §2778 (AECA)
Regulations	Export Administration Regulations, 15 CFR Parts 730-774 (EAR)	International Traffic in Arms Regulations, 22 CFR Parts 120-130 (ITAR)
Control List	Commerce Control List (CCL)	United States Munitions List (USML)
Regulator	U.S. Commerce Department, Bureau of Industry and Security (BIS)	U.S. State Department, Directorate of Defense Trade Controls (DDTC)
Watch Lists	Denied Persons List, Entity List, Unverified List	Debarred Parties List

Fried Frank

Dual-Use Trade Control Basics

Requirements

- Control exports, reexports, technology transfers / deemed exports, activities
  - Dual-use items: items with both military and commercial applications
    - EAR-controlled items classified with Export Control Classification Numbers (ECCNs) on CCL
      - Items without ECCN are classified as EAR99 and generally do not require a license for export
    - Licensing requirements depend on ECCN, destination, intended end use / end user, level of U.S. content, and other considerations
    - *De minimis* rule excludes from EAR control most U.S.-controlled content in non-U.S. items when below certain value thresholds (<10% for embargoed countries; <25% for rest of the world)
    - Encryption technology subject to enhanced licensing and recordkeeping controls, and may be ineligible for *de minimis* treatment in certain cases

Enforcement and penalties

- **Civil:** up to greater of $328,121 or twice the transaction value per incident
- **Criminal:** up to $1 million and / or 20 years imprisonment
- **Administrative:** export suspension / denial (license revocation), ITAR cross-debarment, debarment from government contracts, seized / forfeited commodities, directed compliance

Defense Trade Control Basics

Requirements

- Exports, temporary imports, retransfers, certain activities
  - Defense articles on USML
  - Associated "technical data"
  - Defense services
  - Defense brokering
  - Defense manufacturers, exporters, and brokers must register with DDTC and pay an annual fee
  - Reporting and recordkeeping requirements
- Registration as manufacturer, exporter, or broker
  - 5-day post-closing notice for M&A
  - 60-day pre-closing filing for sale to foreign buyer

Enforcement and penalties

- **Civil:** up to $1, 272,251 per incident relating to export and import controls on defense articles/services
  up to $1,101,061 per incident related to transactions with countries supporting international terrorism
  up to $925,041 per incident related to incentive payments to satisfy offset agreements
- **Criminal:** up to $1 million and / or 20 years imprisonment
- **Administrative:** export suspension / denial (debarment / license revocation), EAR cross-denial, debarment from government contracts, seized / forfeited commodities, directed compliance

Fried Frank

ITAR Compliance Program Guidelines

- In December 2022, DDTC issued ITAR Compliance Program Guidelines, which identify eight key elements of a compliance program:
- **Management commitment:** The guidelines make clear that management commitment is important and recommends the use of an "Export Compliance Management Commitment Statement" signed by senior management
- **DDTC registration, jurisdiction and classification, and authorizations:** An ITAR compliance policy should cover basic information regarding registration, commodity jurisdiction and classification requirements and procedures, the process for obtaining licenses and other authorizations, and other ITAR- controlled activities such as brokering and related activities, such as political contributions, reporting requirements, and cybersecurity and encryption
- **Recordkeeping:** The ITAR requires parties to maintain records related to (a) the manufacture, acquisition, and disposition of defense articles and technical data; (b) the provision of defense services; (c) brokering activities; and (d) information on political contributions, fees, and commissions
- **Detecting, reporting, and disclosing violations:** ITAR registrants should adopt policies and procedures to (a) detect and report ITAR violations; (b) investigate and implement corrective actions; (c) properly submit voluntary disclosures to DDTC; and (d) communicate consequences of ITAR violations to employees
- **ITAR training:** Training should be tailored to address an organization's specific compliance risks and should be reviewed periodically for updates. Training should cover all personnel, with more detailed training for senior management and positions with export functions
- **Risk assessment:** ITAR registrants should implement risk assessments tailored to the organization's ITAR-controlled activity, conducted with regularity, and focused on high-risk areas
- **Audits / compliance monitoring**: ITAR registrants are encouraged to perform comprehensive and independent audits to monitor the effectiveness of their ITAR compliance programs
- **ITAR Compliance manual:** ITAR registrants are encouraged to provide all employees with a complete copy of all of the organization's ITAR compliance policies and procedures

Fried Frank

Export Control Basics: Key Takeaways

- EAR are very broad, but licenses are generally not required for most activities
  - EAR analysis blends decision tree format with due diligence to determine potential licensing requirements—complicated / technical but predictable methodology
  - Even where no license is required, administrative requirements apply (*e.g.*, recordkeeping)
- By contrast, ITAR-controlled activities ***always*** require DDTC authorization (by license or exemption)
  - Exemptions are challenging to use, and are often as or more difficult than obtaining licenses
  - Defense services and other technical data transfers require approved Technical Assistance / Manufacturing License Agreement
  - Retransfer authorization is required for ***any / every*** subsequent transfer to a previously unauthorized
    party or destination
  - **See-through rule:** even the smallest quantum of ITAR-controlled technology in a non-U.S. item remains controlled (unlike EAR, where *de minimis* levels of U.S. content are free of control in many instances)
  - Less predictable and more subject to agency interpretation than EAR

Fried Frank

U.S. Anti-Boycott Regulations

Prohibit U.S. participation in "unsanctioned foreign boycotts"

- Currently limited to the boycott of Israel by Arab League Members and others
- Generally prohibit covered persons from doing or agreeing to:
  - Refuse to do business with Israel or blacklisted companies
  - Discriminate, for boycott reasons, against others based on race, religion, sex, or national origin
  - Furnish information about business relationships with Israel or blacklisted companies

U.S. anti-boycott regimes

- **Commerce Department / EAR (EAR Part 760)**: applies to U.S. persons, their "controlled in fact" subsidiaries, and transactions in the "interstate or foreign commerce of the United States"
  - Prohibits the activities described above
  - Requires reports of boycott-related requests, regardless of action / inaction by recipient

- **Treasury Department / IRS (IRC§999)**: applies to U.S. taxpayers and certain related companies
  - No prohibitions, but certain very important tax benefits denied for cooperation with or participation in Israeli boycott
  - IRS identifies applicable boycotting countries in Federal Register, which currently includes: Iraq, Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, and Yemen

Antiboycott Enforcement

- **In October 2022, BIS released an antiboycott enforcement memorandum**
- **Category A violations:**
  - Discriminating against U.S. persons on the basis of race, religion, sex, or national origin
  - Refusing to do business
  - Furnishing information about race, religion, sex, or national origin of U.S. persons including, but not limited to, providing information in connection with a boycott questionnaire about the religion of employees
  - Evading the antiboycott provisions of the Export Administration Regulations
  - Furnishing information about associations with charitable or fraternal organizations that support a boycotted country
- BIS will begin its penalty calculations for Category A violations at the statutory maximum of $300,000 or twice the value of the underlying transaction
- **Category B violations:**
  - Knowingly agreeing to refuse to do business
  - Requiring, or knowingly agreeing to require, any other person to refuse to do business
  - Implementing letters of credit
  - Furnishing information about business relationships with boycotted countries or blacklisted persons
  - Making recordkeeping violations
- **Category C violation:**
  - Failing to report timely receipt of boycott requests
- BIS intends to more forcefully go after controlled foreign subsidiaries of U.S. companies when they violate BIS' antiboycott regulations, with an emphasis on foreign subsidiaries that make antiboycott requests

Fried Frank

Uyghur Forced Labor Prevention Act

- The UFLPA establishes a **rebuttable presumption** that any items that are mined, manufactured, or produced, wholly or in part, in the Xinjiang Uyghur Autonomous Region (XUAR), or by entities on the UFLPA entities list, are prohibited from importation into the United States
  - "Wholly or in part" means that an item incorporating other items, parts, or materials that are mined, manufactured, or produced in the XUAR are within scope of the UFLPA
  - Importers must provide **clear and convincing evidence** that the items was not mined, produced, or manufactured with forced labor in order to over come the rebuttable presumption
- **Evidence to overcome the rebuttable presumption includes:**
  - Due diligence system information - should include engagement with stakeholders and suppliers, supply chain mapping, a written supplier code of conduct forbidding forced labor, training on forced labor risks, monitoring of supplier compliance, and independent verification, among other things
  - Supply chain tracing information – documentation tracing the supply chain from raw good to finished product
  - Information on supply chain management measures
  - Evidence that goods were not mined, manufactured, or produced in the XUAR
  - Evidence that goods were not produced with forced labor

Uyghur Forced Labor Prevention Act (Cont'd)

- **High priority enforcement areas:**
  - Cotton
  - Tomatoes
  - Polysilicon
- **UFLPA detention and seizure process:**
  - Within 30 days of merchandise being presented at a port of entry, CBP will make a final determination as to whether such merchandise should be excluded, with the failure to take any action being considered an exclusion
    - Accordingly, importers have only 30 days following the presentation of merchandise for examination to overcome the rebuttable presumption importers have only 30 days following the presentation of merchandise for examination
  - Importers who receive a **detention notice** regarding their shipments may respond to the detention notice within 30 days from the date the merchandise is presented for examination to CBP
  - Importers who receive an **exclusion notice** may file an administrative protest within 180 days of receiving the exclusion notice
  - Importers who receive a **seizure notice** may utilize the petition process outlined in 19 C.F.R. Part 171

EXPORT CONTROLS: RECENT DEVELOPMENTS

Russia / Belarus Export Controls

- In response to the Russian invasion of Ukraine in February 2022, BIS amended the EAR to impose significant new license requirements on exports, reexports, and transfers to Russia and Belarus
  - **CCL-based license requirements for Russia** – An export license is now required for all ECCNs in Categories 3-9. Previously ECCNs with unilateral controls (including microelectronics, sensors, telecoms items, navigation equipment, avionics, and aircraft components) did not require a license to Russia
  - **Policy of denial:** Export license applications for Russia will be reviewed, in almost all cases, under a policy of denial. Certain items related to flight safety, humanitarian needs, government space cooperation, and civil telecoms infrastructure are excluded from this policy
  - **Expanded MEU control scope:** All items subject to the EAR except for food and medicine designated EAR99 and 5X992 items not destined for Russian government or SEO use fall within the military end user / end use control scope
  - **Two new foreign direct product ("FDP") rule** that establish EAR control over foreign-produced item
  - A significant narrowing of the situations in which License Exception ENC can be used
- **Applicability to Belarus:** On March 3, 2022, BIS applied the CCL-based license requirements and two new foreign direct product rules to Belarus in addition to Russia
- **Additional export controls at Russia-Ukraine war one-year mark:** Expanded the scope of existing Russian and Belarussian industry sector restrictions related to oil and gas production, commercial and industrial items, and chemical and biological precursors

Fried Frank

Russia Export Controls (Cont'd)

- **Russia FDP Rule:** Controls any foreign-produced item that is not designated as EAR99 and:
  - (i) is a direct product of U.S.-origin technology or software subject to the EAR that is specified in any ECCN in product groups D or E in Categories 3-9 of the CCL, or (ii) is produced by any plant or major component of a plant located outside the United States, when the plant or major component of the plant meets the criteria described in (i)
  - Applies if there is knowledge that the foreign-produced item is destined to Russia or will be incorporated into or used in the production or development of any part, component, or equipment that is not designated EAR99 and is produced in or destined for Russia
- **Russia Military End User FDP Rule:** Controls any foreign-produced item that:
  - (i) Is a direct product of U.S.-origin technology or software subject to the EAR and specified in any CCL categories or (ii) is produced by any plant or major component of a plant where the plant or major component of the plant meets the criteria described in (i)
  - Applies if there is knowledge that it will be incorporated into or used in the production or development of any part, component, or equipment that is produced, purchased, or ordered by any entity with a Footnote 3 designation on the Entity List or if such an entity is involved in the transaction as a purchaser, consignee, or end-user
  - The Russian MEU FDP Rule contains an exception for food and medicine designated as EAR99 and items designed as 5X992 unless destined for Russian government end users or Russian SOEs

Fried Frank

Russia Export Controls (Cont'd)

- **Russia Military End User FDP Rule (Cont'd):**
  - Footnote 3 designations, which indicate that the Russia MEU FDP rule applies to that entity were added to 49 entities
  - BIS has published a list of 32 partner countries that will not be subject to the Russia and Russia-MEU FDP rules because they have adopted or have expressed a willingness to adopt similar rules
- License exceptions: Only the following license exceptions may overcome the Russia FDP Rule and the new CCL-based license requirements:
  - License Exception TMP for items for use by the news media
  - License Exception GOV
  - License Exception TSU for software updates for civil end-users that are wholly-owned U.S. subsidiaries, foreign subsidiaries of U.S. companies that are JVs with U.S. companies, or JVs of U.S. companies with headquarters in Country Group A:5 or A:6 countries, and JVs or wholly-owned subsidiaries of companies headquartered in Country Group A:5 or A:6 countries
  - License Exception BAG, excluding firearms and ammunitions
  - License Exception AVS
  - License Exception ENC for subsidiaries/JVs of U.S. and partner country companies
  - License Exception CCD

Russia Export Controls (Cont'd)

- **Oil refining export controls:** Oil refining equipment listed in Supplement no.4 to Part 746 of the EAR cannot be exported, reexported, or transferred to Russia without a license, regardless of knowledge of its use
  - This license requirement is in addition to the existing restrictions on certain items when the exporter knows or was unable to determine that the item will be used directly or indirectly in exploration for, or production of, oil or gas in Russian deep-water or Arctic offshore locations or shale formations in Russia
  - BIS also changed the license review policy for these oil refining items from a presumption of denial to a more restrictive policy of denial
- **Russia and Belarus License Exception ENC** – This license exception is now only available for civil end-users that are (1) wholly-owned U.S. subsidiaries, (2) foreign subsidiaries of U.S. companies that are joint ventures with other U.S. companies, (3) joint ventures of U.S. companies with companies headquartered in allied countries, (4) wholly-owned subsidiaries of companies headquarter in allied countries, or (5) joint ventures of companies headquartered in allied countries
  - License Exception CDD remains available for certain mass market encryption items exported to Russia

Integrated Circuit Export Controls

- In October 2022, BIS amended the EAR to place new controls on items related to the advanced computing and semiconductor manufacturing industries in China. Specifically, BIS added controls on exports of:
  - Certain types of (i) advanced integrated circuits, (ii) items containing such integrated circuits, (iii) semiconductor manufacturing equipment and (iv) related components, software and technology
  - Certain activities involving (i) advanced node semiconductor fabrication facilities, (ii) semiconductor production equipment and (iii) supercomputers
  - Certain items produced outside of the U.S. when transactions involving such items also involve (i) certain Chinese companies listed on the Entity List that are subject to a new Footnote 4 designation, (ii) supercomputer-related activities in China or (iii) advanced computing applications in China
  - U.S. person activities related to the development or production of (i) integrated circuits at semiconductor fabrication facilities in China and (ii) specific types of semiconductor production equipment in China
- BIS has instituted a resumption of denial licensing policy for exports of RS-controlled items to integrated circuit fabricators in China
- BIS also added 31 Chinese entities to the Unverified List

Fried Frank

Recent Export Control Updates

- Changes in the *de minimis* level applicable to Cuba and tightening rules for donations to Cuba
  - When Cuba was removed from the List of State Sponsors of Terrorism in 2015, foreign-manufactured items exported to Cuba would only be subject to the EAR if they contained 25% or greater controlled U.S.-origin content. With Cuba readded to the list, the *de minimis* threshold is now 10%
  - License now required for humanitarian donations to organizations administrated or controlled by the Cuban government or communist party
- DDTC cloud computing rule published in January 2020. Per this rule, sending, taking, or storing ITAR-controlled technical data is not an export as long as the data is:
    - Unclassified
    - Secured using end-to-end encryption
    - Secured using cryptographic modules compliant with FIPS 140-2 or its successors
    - Not intentionally sent to a person in or stored in a country subject to U.S. arms embargoes or the Russian Federation
    - Not sent from a country subject to U.S. arms embargoes or the Russian Federation
- Emerging and Foundational Technologies Export Controls
- New restrictions on Chinese, Russian, and Venezuelan military end-users / end-use
- BIS reduces encryption reporting requirements for mass market chips, chipsets, and electronic assemblies

Fried Frank

MEU Rule / MEU List

- In April 2020, BIS published two final rules tightening restrictions on exports of technologies to military end-users in China, Russia, and Venezuela
  - A BIS license is required to export, reexport, or transfer certain items (listed at Supplement No. 2 to Part 744 of the EAR) if a party knows or has reason to know that the item is intended for a military end-user or a military end use
  - **Exporters are responsible for conducting their own due diligence** to determine if an entity is a military end-user or if an export is intended for a military end use
  - A license is required for exports to an MEU even if the item is not intended for a military end-use
- In 2021, BIS published rules adding **Myanmar** and **Cambodia** to the list of countries subject to the military-intelligence end-user and end-use controls
- BIS also removed License Exception CIV and now requires a license for national security-controlled items countries of national security concern (Country Group D:1)
- In December, 2020 BIS published a Military End User List (MEU List)
  - The MEU List is not exhaustive
  - An entity on the MEU List is one that BIS definitively considers to be an MEU. Non-listed parties could still be military end-users
- **Military Intelligence End User (MIEU) Rule:** In January 2021, BIS published a rule imposing license requirements for items subject to the EAR that are intended for end-users or end-uses related to the intelligence activities of the Chinese, Russian, and Venezuelan militaries

Fried Frank

Emerging and Foundational Technologies

- On November 19, 2018, BIS issued an advance notice of proposed rulemaking (ANPRM) relating to export controls on emerging technologies, and has since published a series of new controls
- The newly controlled technologies are primarily items used in semiconductor manufacturing, as well as surveillance equipment and certain spacecraft
  - Hybrid additive manufacturing (AM) / computer numerically controlled (CNC) tools
  - Computational lithography software designed for the fabrication of extreme ultraviolet (EUV) masks
  - Technology for finishing wafers for 5nm production
  - Digital forensics tools that circumvent authentication / authorization controls on a computer (or comms device) and extract raw data
  - Software for monitoring and analysis of communications and metadata acquired from a telecommunications service provider *via* a handover interface
  - Sub-orbital craft
- On October 5, 2021, BIS published new a final rule placing new controls on genetic editing software
- Other categories of emerging technologies identified in the 2018 ANPRM include biotechnology, artificial intelligence and machine learning, microprocessors, advanced computing, data analytics, quantum information and sensing, additive manufacturing, and robotics, among others
- The categories are broad and BIS has significant flexibility in determining which items from these categories to control
- BIS has focused on obtaining support for multilateral controls over speed of implementation

Fried Frank

Emerging and Foundational Technologies (Cont'd)

- On August 27, 2020, BIS issued a ANPRM relating to export controls on foundational technologies, similar to the previous ANPRM on emerging technologies
- Unlike the emerging technologies ANPRM, the foundational technologies ANPRM does not describe specific categories of technology, but notes that the term foundational technologies includes "commodities" and "software," in addition to technology
- BIS is not seeking to expand jurisdiction over technologies that are not currently subject to the EAR, such as "fundamental research"
- Examples of potential foundational technologies identified in the ANPRM:
  - Items such as semiconductor manufacturing equipment and associated software tools, lasers, sensors, and underwater systems that can be tied to indigenous military innovation efforts in China, Russia or Venezuela
  - Items that are currently classified at the AT level or as EAR99 but that may warrant review to determine if they are being utilized or required for innovation in developing conventional weapons, enabling foreign intelligence collection activities, or weapons of mass destruction (WMD) applications.
  - Technologies that have been the subject of illicit procurement attempts which may demonstrate some level of dependency on U.S. technologies to further foreign military or intelligence capabilities, or the development of WMDs

Huawei Added to the Entity List

- BIS added Huawei and numerous foreign subsidiaries to the Entity List in May 2019 because "there is reasonable cause to believe that Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States." Currently over 150 Huawei affiliates are designated on the Entity List
  - Additional non-US affiliates of Huawei were added to the Entity List in August 2019, May 2020, and August 2020
- Exports of all items subject to the EAR to Huawei require an export license, including certain technical exchanges and no license exceptions are available
- Huawei is a major customer for many U.S. technology companies (*e.g.*, semiconductor companies) and a participant in several standards setting and certification bodies
- As of April 2021, BIS approved 113 export licenses involving Huawei out of 169 applications received for an approval rate of 69%
  - Only two applications were denied outright and the remainder were returned without action, likely due to missing required information
- The Huawei designation and its potential resolution highlight the confluence of (and potential conflicts between) U.S. trade and national security policy

Huawei Added to the Entity List (Cont'd)

- In November 2021, BIS announced its first enforcement case against a company (SP Industries) for unauthorized exports to Huawei of EAR99 items
    - SP Industries cooperated with BIS and voluntarily self-disclosed two of the violations and reached an $80,000 settlement agreement
- As evidenced by the Huawei designations, the Department of Commerce has increasingly used Entity List designations as a foreign policy tool
- BIS amended the Foreign Direct Product Rule and applied it to Huawei and Huawei's affiliates. Under the Foreign Direct Product Rule, foreign-produced items made with less than the *de minimis* amount of U.S. content will still be subject to the EAR
    - This rule prohibits the transfer to Huawei of any foreign-produced item that is (a) the direct product of specified software or technology subject to the EAR, or
    - (b) produced by a plant or major component of a plant that is itself the direct product of U.S.-origin software or technology
- The Foreign Direct Product Rule applies to any transaction where Huawei is the end-user, purchaser, or an intermediate or ultimate consignee
- In April 2023, BIS imposed a $300 million civil penalty on Seagate for FDP Rule violations related to the sale of hard drive disks to Huawei after it was added to the Entity List

Fried Frank

EXPORT CONTROLS: ENFORCEMENT CASE STUDIES

Enforcement Case Studies (BIS)

Seagate Technology LLC and Seagate International Headquarters Pte. Ltd. ("Seagate") (April 19, 2023)

- Seagate received an unprecedented $300,000,000 fine for violations of the EAR related to exporting hard drive disks ("HDDs") to Huawei in violation of the EAR, following Huawei's Entity List designation and the promulgation of the Foreign-Produced Direct Product Rule
- On May 16, 2019, Huawei and certain of its affiliates were added to the Entity List
- On August 17, 2020, BIS imposed a license requirement on certain foreign-produced items when (1) there is knowledge that a listed Huawei entity is a party to the transaction and (2) the foreign-produced item is produced by an overseas plant or major component of a plant that is itself a direct product of U.S.-origin technology or software subject to the EAR ("FDP Rule")
- While the two other major supplies of U.S.-origin HDDs swiftly and publicly announced that they would cease selling HDDs to Huawei, in September 2020, Seagate announced that it would continue to do business with Huawei, becoming its sole supplier of HDDs
- Between August 2020 and September 2021, Seagate exported or caused to be exported more than 7.4 million HDDs subject to the FDP rule without BIS authorization. The HDDs were valued at over $1.1billion
- Between January and September 2021, Seagate US extended Huawei multiple lines of credit totaling more than $1 billion, allowing Huawei to obtain a volume of HDDs it would not have otherwise been able to obtain

Enforcement Case Studies (BIS) (Cont'd)

- Throughout the time of the violations, Seagate's senior leadership maintained that its HDDs were outside the scope of the FDP Rule and Seagate did not need to obtain a specific license in order to make sales to and export its HDDs to Huawei
- Seagate had HDD manufacturing sites in China, Northern Ireland, Malaysia, Singapore, Thailand, and the United States. Seagate used equipment, including testing equipment, subject to the EAR and the FDP rule, including:
  - An automated laser-based surface inspection system that was classified as 3B992 and was the direct product of U.S.-origin E3991 technology
  - Iron Beam Etch and Iron Beam Deposition technology that was classified as 3B992 and was the direct product of U.S.-origin E3991 technology
  - Both items were essential and thus considered a major component of Seagate's HDD plants
- For its EAR violations, Seagate was assessed a civil penalty of $300,000,000, payable in quarterly installments of $15 million over five years. The first payment is due Oct. 31, 2023
  - Seagate is also required two complete three audits of its export controls compliance program. The first audit is required to be an external audit and the remaining two will be internal audits
  - Seagate is subject to a five-year denial of its export privileges, with the denial suspended for a period of five years, provided that Seagate complies with the terms of the civil penalty

Enforcement Case Studies (DDTC)

Honeywell International (April 27, 2021)

- Honeywell sent RFQs to U.S. and foreign suppliers and included export-controlled drawings of parts that suppliers were asked to provide quotations for included
- There were 71 ITAR-controlled drawings (of various aircraft, tanks, missiles, and engines) that were exported to Canada, Ireland, China, and Taiwan without appropriate authorizations
- In a separate set of incidents in 2018, Honeywell employees without authorization exported technical drawings using a different file exchange system in order to speed up the procurement process

- **Aggravating Factors**
  - Some of the drawings contained technical data designated as SME, a designation used for articles for which special export controls are warranted due to their capacity for substantial military utility or capability
- **Mitigating Factors**
  - Honeywell made fully voluntary disclosures in September 2016 and September 2018
  - After the first disclosure, Honeywell took multiple corrective actions to prevent similar violations in the future
- **Penalty**
  - $13,000,000 settlement agreement with $5M suspended on the condition that it be used for remedial compliance measures
  - Various remedial measures including a strengthened compliance program, training, automated export compliance system, at least one outside audit
  - Because of the remedial measures Honeywell agreed to, DDTC decided not to impose administrative debarment

Fried Frank

Enforcement Case Studies (DDTC) (Cont'd)

Airbus SE (Jan 29, 2020)

- From 2011-2017, Airbus sought authorization for the export of defense articles and provision of defense services with respect to the C-295 military transport aircraft without providing accurate Part 130 statements for sales to the armed forces of Colombia, Egypt, Ghana, Jordan, Indonesia, Kazakhstan, Mexico, Poland, and Vietnam
- Airbus was required to provided Part 130 reports identifying fees or commissions paid, offered, or agreed to be paid, in order to facilitate these sales
- Airbus lacked a system for maintaining records related to the information necessary to provide Part 130 reports

- **Aggravating factors**
  - Significant compliance program deficiencies and a lack of internal controls despite identifying Part 130 as a risk area
  - Inadequate processes undertaken by the ITAR Empowered Official to verify the accuracy of Part 130 statements
  - Uneven recordkeeping contributing to systemic failure to provide accurate Part 130 reports
- **Mitigating Factors**
  - Airbus' cooperation with Department of State's request
  - Airbus' history of voluntarily disclosing violations
  - Airbus' efforts to mitigate the harm to U.S. national security and foreign policy caused by its violations
- **Penalty**
  - $10,000,000 settlement agreement with $5M suspended on the condition that it be used for remedial compliance measures
  - Remedial measures including strengthened compliance policies and at least two outside audits

Fried Frank

Enforcement Case Studies (BIS) (Cont'd)

SAP SE (April 29, 2021) (BIS civil penalty + OFAC settlement + DOJ non-prosecution agreement)

- SAP and SAP Partners sold SAP software licenses and maintenance agreements to foreign-registered pass-through entities that were shell corporations located outside of Iran that conducted business in Iran and were affiliated with Iranian companies and
- From Dec. 2009 through Sept. 2019, end-users in Iran utilized the pass-through entities to make 24,634 downloads of SAP software products, upgrades, and patches (ECCN 5D002 and EAR99)
- SAP had conducted audits of its export controls processes and a 2006 audit reported that SAP was not identifying the country to which on-prem software was being downloaded. Subsequent audits in 2007, 2010, 2014 also revealed issues, including a lack of IP screening and geo-location blocking
- SAP did not activate geo-location blocking until 2014
- SAP received whistleblower reports alleging sales by SAP Partners to foreign-registered affiliates of Iranian customers

Enforcement Case Studies (BIS) (Cont'd)

SAP SE (Cont'd)

- **Mitigating factors (as identified by OFAC)**
  - SAP had no prior sanctions violations in the five years preceding the date of the earliest violations
  - SAP substantially cooperated with OFAC's investigation
  - SAP took significant remedial actions including terminating accounts, blocking downloads, developing and implementing improved geolocation IP screening, terminating employees who knowingly engaged in prohibited sales or vailed to adhere to internal policies
- **Aggravating Factors (as identified by OFAC)**
  - SAP demonstrated reckless disregard and failure to exercise a minimal degree of caution by failing to act on the findings of multiple internal audits
  - SAP also acted recklessly by not having a compliance program commensurate to its size and sophistication
  - SAP had direct knowledge or reason to know that SAP software and cloud services were being sold to or used by entities and end-users in Iran and were supported from the United States
  - SAP's violations caused harm to U.S. sanctions program objectives and undermined U.S. policy
  - SAP is a sophisticated software company with significant international operations
- **Penalty**
  - OFAC and SAP reached a settlement for **$2,132,174**
  - BIS imposed a **$3,290,000** civil penalty (taking into account the NPA and OFAC settlement)
  - BIS required SAP to complete three internal audits of its export controls compliance program

Fried Frank

Michael T. Gershberg



Michael T. Gershberg

Partner
Washington, DC
T:+1.202.639.7085
michael.gershberg@friedfrank.com

Michael T. Gershberg represents foreign and domestic clients regarding the application of economic sanctions, export control laws and regulations, and the CFIUS review process.

Much of Michael's work involves offering practical guidance on the Export Administration Regulations (EAR), International Traffic in Arms Regulations (ITAR), and economic sanctions administered by the Office of Foreign Assets Control (OFAC). Clients also seek Michael's counsel in connection with their obligations under the anti-boycott and anti-money laundering rules.

Clients of Michael's export control and economic sanctions practice rely on his advocacy before governmental agencies, and turn to him to conduct internal investigations and prepare voluntary self-disclosures and other legal submissions. Michael also assists clients in connection with export transactions and enforcement issues, due diligence for mergers and acquisitions, economic sanctions and export control training, determining export jurisdiction and classification, developing compliance plans and providing compliance counseling, and export licensing.

Michael also advises clients concerning regulatory issues related to foreign investment transactions, including proceedings before the inter-agency Committee on Foreign Investment in the United States (CFIUS). Foreign investors and US sellers engage his representation throughout the CFIUS process, from negotiating CFIUS risk allocation with transaction counterparties to preparing CFIUS filings and negotiating mitigation agreements. Michael also advises public and private companies and investment managers regarding CFIUS jurisdiction and national security risk, and he prepares related provisions in M&A transaction agreements and private fund formation documents.

Chambers Global and *Chambers USA* recognize Michael among the world's leading lawyers for business in International Trade: Export Controls & Economic Sanctions, where clients enthuse "Michael is an excellent attorney and is super responsive," "his expertise in trade compliance is invaluable," and "his deep experience in sanctions and export compliance and his ability to break down complex concepts are his individual strengths." Other clients note that "Michael is a key provider of advice with respect to economic sanctions," and "he is commercially oriented and knows his stuff." Michael has also been named by *Chambers USA* as a "Recognized Practitioner" in International Trade: CFIUS Experts, and he was selected as a "Global Leader" by *Who's Who Legal: M&A and Governance* in the Foreign Investment Review Chapter. Michael was also named a 2019 *Law360* "MVP" in International Trade. Additionally, Michael has been named in *Thomson Reuters* 2023 Stand-Out Lawyers List.

Michael is the editor of the *ITAR Enforcement Digest* and a contributor for the CFIUS chapter of the *M&A treatise Takeover Defense: Mergers and Acquisitions*. He is also a co-author of *Fried Frank's International Trade and Investment Alert®*, which reports on significant developments regarding CFIUS, economic sanctions, export controls, and other regulatory compliance matters affecting business activities.

Fried Frank

Attorney advertising. Prior results do not guarantee a similar outcome.

Fried Frank