UNDERSTANDING OFAC

A Best Practices Compliance Guide for All Businesses

INTRODUCTION

Every year, the U.S. Treasury Department casts a wider net of Office of Foreign Assets Control (OFAC) violations, ensnaring everyone from unwitting small businesses to sophisticated corporations. The continual expansion of a global economy that trades increasingly online, across international borders and through digital currency is driving the Treasury's dedicated efforts to ensure all U.S. businesses, including any foreign subsidiaries, comply with OFAC regulations that aim to thwart illicit activity and terrorism.

Recently, the Treasury's efforts gained even more steam when OFAC issued an official sanctions compliance program (SCP) framework for the first time. A Framework for OFAC Compliance Commitments was published on May 2, 2019, and shortly thereafter, OFAC began regularly referencing this framework in its enforcement actions (EAs).

OFAC's Mission

OFAC enforces economic and trade sanctions based on U.S. foreign policy and national security goals. These sanctions, imposed against targeted foreign countries and regimes, terrorists, international narcotics traffickers, and those involved in the proliferation of weapons of mass destruction (WMDs), help protect U.S. national security, our foreign policy and economy.

The Result of Increased OFAC Scrutiny:

- A single OFAC fine now usually equals, or even dwarfs, the total amount of fines OFAC once levied in a full year.
- Other business types are just as likely as traditional banks to incur large citations, including seven–, eight– and nine– digit fines.
- The smallest fines imposed today are significantly higher than those of just five years ago.

Once known almost exclusively to financial institutions, OFAC awareness has permeated the general marketplace as well. But as our analysis of OFAC enforcement actions shows, a remarkable number of businesses still do not have any type of OFAC compliance program in place, despite risk profiles that call for one. And wholly inadequate or ignored OFAC compliance programs still abound among those who do understand the need to screen transactions against the OFAC Specially Designated Nationals (SDN) list, a list of individuals and entities with whom all U.S. citizens and businesses are prohibited from doing business.

This white paper examines OFAC compliance by outlining the Treasury's *A Framework for OFAC Compliance Commitments* and identifying best practices to help all business and industry types better understand and meet their OFAC compliance obligations, thereby avoiding costly penalties, damaged corporate reputations and even potential criminal charges.

OFAC's SANCTIONS COMPLIANCE FRAMEWORK

In its A Framework for OFAC Compliance Commitments, OFAC reiterates the need for a risk-based SCP based on a "company's size and sophistication, products and services, customers and counterparties, and geographic locations." OFAC also specifically calls for an SCP framework that consists of these five essential components:

1. **Management commitment:** Senior management reviews and approves the SCP, provides adequate resources and sufficient authority and autonomy to the compliance unit, appoints a dedicated OFAC sanctions compliance officer, promotes a "culture of compliance" and recognizes the seriousness of violations.
2. **Risk assessment:** The risks posed by clients, customers, products, services, supply chain, intermediaries, counterparties, transactions and geographic locations are assessed and inform the extent of due diligence, including at key points such as onboarding and mergers or acquisitions.
3. **Internal controls:** Organizations have written policies and procedures that adequately address their risk assessment findings and are communicated and enforced.
4. **Testing and auditing:** Whether conducted internally or by an external party, the OFAC testing and auditing functions are independent, accountable to senior management, reflect the organization's risk profile and immediately address negative test results.
5. **Training:** On at least an annual basis, all appropriate employees are trained on their job specific OFAC responsibilities and continuously held accountable for them.

Every enforcement action in 2020 included a reference to this framework, which further indicates OFAC's intention to hold organizations subject to U.S. sanctions compliance accountable to it.

"OTHER BUSINESSES" FINED BY OFAC FAR OUTNUMBER TRADITIONAL BANKS

From 2006 through 2020, OFAC imposed $5.68 billion in civil money penalties (CMPs). While banks still typically incur the highest dollar fines, CMPs against businesses other than banks, including non-traditional financial institutions as defined by the USA PATRIOT Act, make up the majority of the total number of fines every year.

In each of the last 12 years, other businesses represented close to or over 75 percent of the total number of all OFAC fines imposed. And in five of those years, the total number of fines against other businesses was over 80 percent.

Comparing the Percentage of Fines Between Traditional Banks & All Other Businesses

Year	% of Fines Against Traditional Banks	% of Fines Against All Other Businesses, Including Fintechs
2020	19%	81%
2019	23%	77%
2018	29%	71%
2017	19%	81%
2016	11%	89%
2015	33%	67%
2014	26%	74%
2013	26%	74%
2012	31%	69%
2011	14%	86%
2010	22%	78%
2009	11%	89%

A Closer Look at Regulatory Fines over the Last 12 Years

OFAC violations are costing U.S. businesses hard-earned cash. A further look into the 12-year average percentage of CMPs levied against the All Other Businesses category shows that the biggest concentration in fines is those from $100,000 to $499,999 (28 percent). However, in 2016, 2018 and 2019, fines over $1 million earned the top spot as the largest fine category. That fact, along with the trends in this chart, indicate that OFAC fine amounts are rising as quickly as its reach is expanding beyond traditional banks.

Percentage of OFAC Fines by Dollar Amount Per Year for All Other Businesses

Year	Over $1 million	$500,000 to $1 Million	$100,000 to $499,999	$50,000 to $99,999	$25,000 to $49,999	Less Than $25,000
2020	25%	25%	31%	6%	0%	13%
2019	**38%**	11.5%	35%	7.5%	4%	4%
2018	**60%**	0%	20%	20%	0%	0%
2017	25%	19%	37.5%	6%	0%	12.5%
2016	**37.5%**	12.5%	**37.5%**	0%	12.5%	0%
2015	10%	10%	30%	20%	20%	10%
2014	29%	6%	24%	17.5%	17.5%	6%
2013	15%	5%	35%	10%	15%	20%
2012	18%	0%	46%	9%	9%	18%
2011	5.5%	5.5%	16.5%	5.5%	17%	50%
2010	19%	9.5%	9.5%	9.5%	9.5%	43%
2009	8%	0%	17%	4%	17%	54%
12-Year Avg	**24%**	**9%**	**28%**	**10%**	**10%**	**19%**

The statistics provided in the paragraphs and charts in this section were gleaned from an extensive review of OFAC's Enforcement Actions by Year on the U.S. Treasury's website, for the years 2006 through 2020.

Multimillion-Dollar Fines for Other Businesses Becoming More Common

For a business of any size, these fine amounts can cause considerable damage; for a smaller business, they can spell catastrophe. Then imagine the havoc created by these multimillion-dollar CMPs levied against a wide variety of industries:

- Telecommunications Company: $100.9 million
- Aerospace Services Provider: $50.9 million
- Technology Company: $12 million
- IT Services Company: $7.8 million
- Manufacturer: $7.77 million
- Money Services Business: $7.66 million
- Pharmaceutical Firm: $7.62 million
- Oil/Energy Provider: $5.97 million
- Two Travel Services Providers: $5.9 million each
- A Chemical Manufacturer: $5.5 million
- Agriculture/Seed Company: $4.32 million
- Two well-known Multinational Conglomerates: $4.1 million and $2.7 million
- Manufacturer: $4.07 million
- Travel Services Provider: $2.8 million
- Oilfield Services Provider: $2.77 million
- Manufacturer: $2.06 million
- Oil and Gas Company: $2 million

HOW OFAC APPLIES TO VARIOUS INDUSTRIES

Every U.S. citizen, permanent resident alien and company, as well as any overseas branch of the same, is prohibited from doing business with those targeted on OFAC's SDN List, which includes terrorists, narcotics traffickers and those controlled by or acting on behalf of sanctioned countries.

The USA PATRIOT Act Broadens "Financial Institution" Definition

Since the attacks of Sept. 11, 2001, OFAC's role in national security has increased multi-fold. The passage of the USA PATRIOT Act brought with it a broader definition of the term "financial institution" in order to highlight industries that, by their very nature, are at higher risk for money laundering and OFAC violations. Those industries include the following:

Vehicle Dealers and Vehicle Parts Suppliers

Under the USA PATRIOT Act, automobile, boat and motorcycle dealers are deemed "financial institutions" because OFAC knows that sanctioned parties can easily launder money through the purchase of such vehicles. Therefore, vehicle dealers must be aware of cash transactions that could indicate an SDN avoiding the U.S. financial system and eluding detection by transporting the vehicle elsewhere for easy liquidation. That, however, is not the only issue.

Airplanes and their parts are critical for terrorists and other sanctioned entities, allowing them to run their operations and expand their organizations beyond isolated areas. A large aerospace services provider was fined $50.9 million dollars for re-exporting aircraft parts. Despite its size and international reach, this corporation did not have a formal OFAC compliance program in place, which was noted by OFAC.

In addition, vehicle and airplane dealers and suppliers must be aware of the ultimate destination of their products. A truck supplier was fined $1.7 million for selling 63 trucks to customers in Europe "that it knew or had reason to know were ultimately intended for buyers in Iran." Meanwhile, an aircraft dealer was fined $210,600 for leasing three aircraft engines to a customer in the United Arab Emirates, who subleased them to a Ukrainian airline, which installed them on planes leased to a sanctioned entity in a third country.

Organizations dealing in vehicles and parts must also consider all business operations when it comes to OFAC compliance. A car dealer, who also finances auto loans, was dealt a $23,400 CMP for extending a loan to an SDN. And a boat dealer learned that OFAC's country-based sanctions prohibit almost all business activity with those countries. It was fined $13,500 after entering into a contract to sell boats in a sanctioned country.

Every U.S. citizen, permanent resident alien and company, as well as any overseas branch of the same, is prohibited from doing business with those targeted on OFAC's SDN List.

Casinos

Casinos, by their nature, deal mostly in cash. And as an added amenity, many offer house accounts allowing casino guests to safeguard their cash. SDNs like this feature because it puts their cash outside of the traditional financial system, which is why OFAC is concerned about these accounts and why the USA PATRIOT Act considers casinos offering such house accounts to be financial institutions. While any house account transaction could include an OFAC violation, there are certain scenarios that indicate a higher risk, including when a casino guest deposits a large sum of cash into such an account, and later withdraws it without any use in between.

Insurance

Due to its broad scope and billions of customers, including many commercial ones with large group policies, the insurance industry is particularly vulnerable to OFAC violations. OFAC explicitly warns that no one in this industry, including underwriters, agencies, carriers, brokers, primary insurers, re-insurers and U.S. citizens of foreign insurance companies, are allowed to provide any services to an SDN or a sanctioned country without a license. CMPs continue to be levied against members of this industry for not heeding that clear warning:

- Processing claims without a license for persons in a sanctioned country cost an insurer $348,000
- Dealing in property of a specially designated narcotics trafficker resulted in a $345,315 fine for an insurer
- Insuring a corporation's risks in a sanctioned country cost one insurer $279,038 and another $35,211
- Issuing coverage for flagged vessels earned a marine insurer a $271,815 CMP
- Providing coverage to sanctioned individuals through group policies and paying related claims in a sanctioned country cost a health insurance provider $128,704
- Issuing a death benefit to a beneficiary in a sanctioned country cost an insurer $22,500
- Providing a car insurance policy to an SDN cost an auto insurer $11,000

One 2017 enforcement action against this industry stands out. A large, multi-national carrier was fined $148,698 for insuring maritime shipments of goods to sanctioned countries. The enforcement action indicated that the company's "OFAC compliance program in place at the time of the apparent violations included recommendations for when to use exclusion clauses in the policies it issued regarding coverage or claims that implicated U.S. economic sanctions." It went on to state that the majority of the company's policies included such exclusionary clauses, but "most were too narrow in their scope and application to be effective."

This particular enforcement action culminated in a cautionary statement for the industry: "This enforcement action highlights the important role that properly executed exclusionary clauses and robust compliance controls play in the global insurance industry's efforts to comply with U.S. economic sanctions programs."

Real Estate and Construction-related Firms:

Anyone involved in real estate, including real estate or settlement agents and title insurance or escrow companies, is prohibited from engaging in any transaction involving an SDN and is required to freeze any SDN assets placed in their accounts. This is true for new purchases, refinances and any other real estate dealings. Even homeowners' associations are liable for OFAC violations, as a $9,000 CMP proved in a case where an association used the proceeds of the sale of an SDN's real property.

This sector also extends to construction-related organizations, as the following examples demonstrate: an architecture firm fined $140,400 for providing design services for a hotel in a sanctioned country and a construction material supplier fined $506,250 for buying products originally sourced from a sanctioned country.

Even homeowners' associations are liable for OFAC violations, as a $9,000 CMP proved in a case where an association used the proceeds of the sale of an SDN's real property.

Travel and Tourism:

There have been four multimillion-dollar fines levied against travel services providers since 2006, along with several smaller, but not insignificant, fines. Interactions between a travel agent and an SDN can be as obvious as the purchase of travel services; however, there are other, more obscure interactions that travel agents, ticket agents, tour companies, airline companies, hotel operators and even event promoters must be on guard against, including the following:

- International travel company fined $5.99 million for processing unauthorized travel-related services
- Travel assistance company fined $5.86 million for providing services in a sanctioned country
- Travel agency fined $5.2 million for booking travel to a sanctioned country
- Major travel services firm fined $2.8 million for booking flights to, and hotels in, a sanctioned country
- Hotel chain fined $735,407 due to an acquisition, which included two hotels in a sanctioned country
- Two travel companies fined $325,406 and $222,705 for providing accommodations in sanctioned countries
- Tour provider fined $43,875 for providing travel-related services without OFAC authorization
- Event promoter fined $48,600 for paying an individual in a sanctioned country for one of its events

Importers and Exporters:

In OFAC terms, this category covers a broad array of businesses, and may include yours if it has any involvement whatsoever in importing or exporting goods or services. OFAC examines four factors when investigating possible import or export violations:

- **Destination:** Is the export going to, or is the import coming from, a sanctioned country?
- **End User:** Are ANY of the parties who will use the product named on the SDN list?
- **Sales Servicers:** Is ANY party to the transaction (shipper, insurer, bank, etc.) named on the SDN List, even if the transaction is otherwise legitimate?
- **End Use:** Will the product be used for legitimate purposes or could it be used for terrorism, narcotics trafficking or in the proliferation of WMDs?

An analysis of EAs over the last few years reveals just how innocuous some of the exported products involved in OFAC violations seem on the surface. In each case, the goods were exported to a sanctioned country, and in some cases, the exports were likely eligible for an OFAC special license had the company applied for it:

- Pharmaceutical lab fined $7,617,150 for exporting surgical products
- Dental equipment firm fined $1,220,400 for selling goods to distributors dealing in a sanctioned country
- Small medical supply firm fined $515,400 for “willfully” exporting goods to a sanctioned country
- Cosmetics firm fined $450,000 for exporting nail care products (valued at $33,299)
- Medical supply company fined $404,100 for exporting unlicensed medical goods

The Treasury Department also sent this industry a cautionary statement in a recent enforcement action, which carried a $372,465 fine against a U.S. company and its Canadian subsidiary: “This enforcement action reinforces certain compliance obligations for U.S. persons, including U.S. parent corporations that maintain subsidiaries located outside of the United States, as well as their U.S. person employees.”

Jewelry, Precious Gem and Metal Dealers:

The unique characteristics of these items are what keep dealers of the same on OFAC's radar: they hold their value, are easily concealed and transported, and quickly liquidated. Dealers should be wary of all cash transactions. Also, for wholesale transactions, they must know where the merchandise originates from or where it is being exported to, i.e., a sanctioned country or entity.

For example, a jewelry and luxury goods dealer was fined $344,800 in a case where the information and documentation provided to the company about the buyer matched the name, address and country location on the SDN list, but the company "did not identify any sanctions-related issues with the transaction prior to shipping the goods."

In addition, some merchandise sources may require a deposit from a dealer. A pearl and gem dealer was fined $25,000 for this type of transaction because the intended recipient of the funds transfer was a blocked entity. Dealers in gold and silver also must be careful of providing transactional accounts for their clients, a practice that cost one dealer $2.95 million because an SDN was involved.

Money Services Businesses (MSBs):

Mortgage companies, card services companies, and providers and sellers of Prepaid Access all are in the business of providing cash or credit. SDNs and Specially Designated Narcotics Traffickers (SDNTs) need to finance their activities. Knowing that traditional banks have extensive OFAC compliance programs, many turn to MSBs. Failing to screen for potential OFAC matches, no matter how small the transaction, can result in an MSB opening a credit card account or processing other transactions for an SDN or SDNT.

One MSB was fined $401,697 because one of its agent banks established a sub-agent relationship with a sanctioned entity. Other recent fines against MSBs range from $8,720 to $40,160.

Non-profits and Charities:

Groups falling into this category must be aware of OFAC sanctions programs for a number of reasons. First, if such an entity wants to provide humanitarian aid to a sanctioned country as part of its outreach program, it must apply for an appropriate license. Second, if the group wants to export goods or services, it must ensure it is not dealing with a sanctioned individual, entity or country. And finally, because terrorist groups have been known to start charities or exploit existing ones as a way to raise and move funds or otherwise support their organizations, legitimate charities need to screen out such activity.

In one instance, a well-established non-profit was fined $780,000 for "knowingly and willfully" transferring funds to sanctioned countries; and in another, the director of a small nonprofit foundation was individually fined $10,000 for "unauthorized travel-related transactions during business travel" to a sanctioned country.

Other Disturbing Trends in OFAC Fines Emerge in the Last Few Years

A thorough review of recent years' OFAC enforcement actions uncovers four other disturbing trends.

1. OFAC is increasingly fining U.S. companies for actions that occurred at their foreign subsidiaries. Such violations accounted for 30 percent of CMPs in 2019 and 25 percent in 2020.
2. OFAC is going after small businesses with as much gusto as larger, more sophisticated firms. This was particularly true in 2014 and 2015, when OFAC specifically identified the fined entity as a "small business" in 21 percent of its enforcement actions.
3. An alarming number of enforcement actions noted that no OFAC compliance program was in place at the time of the violation. In the following years, the percentage of enforcement actions falling into this category amounted to:
    - **2018:** 14 percent
    - **2017:** 25 percent
    - **2016:** 55 percent
    - **2015:** 40 percent
    - **2014:** 43 percent
4. Beyond the industries outlined above that have earned the "financial institution" designation under the USA PATRIOT Act, there are several other industries that are quickly and increasingly becoming the target of OFAC investigations and fines.

Energy and Fossil Fuel-related Firms:

Of late, there has been a noted uptick in enforcement actions against energy and fossil fuel-related firms. For instance, in 2016, 33 percent of all fines were levied in this category, as firms providing oilfield services, engaging in oil and gas exploration and delivering equipment for oil and gas exploration felt the combined sting of $6.89 million in CMPs. OFAC notes that many regions in which such firms interact are those having high sanctions risk, and they are required to take appropriate precautions. In addition, energy and fossil fuel-related activity is likely to provide significant economic benefit to the sanctioned country, in direct opposition to OFAC sanctions objectives.

Other recent examples of fines in this industry include the following, all of which were levied against firms that OFAC described as large, sophisticated and globally experienced. In other words, they should have known better.

- Exporting oil field services with an "ineffective and easily circumvented" compliance program cost one firm $2.77 million
- Dealing in blocked services with the knowledge of senior management cost a second firm $2 million
- Producing and presenting analytical reports for oil exploration in a sanctioned country's territorial waters resulted in a $441,366 fine for an offshore oil engineering firm
- Exporting oil rig supplies in sanctioned areas cost another firm $415,350
- Re-exporting goods to a sanctioned area resulted in a fine of $17,500 for yet another

Technology (Hardware, Software, Networking and Data Processing Services):

The explosive growth of the technology sector has come at a high price, including the largest OFAC fine ever imposed against a non-bank entity: $100.9 million against a “sophisticated and experienced” telecommunications company operating with a “non-existent or unenforced” OFAC compliance program. Additional examples include the following:

- Technology company, which was “engaging in, and systemically obfuscating, conduct it knew to be prohibited,” was hit with a $12,027,066 fine
- Telecom company that provided commercial services and software to a specially designated global terrorist (SDGT) had to pay $7.8 million
- Another telecom company exported satellite equipment to a sanctioned entity and was fined $894,111
- Wireless data communications firm, operating without an OFAC compliance program, fined $504,225
- Technology firm was fined $473,157 after a foreign entity it acquired failed to stop selling equipment to a sanctioned country and took active measures to hide it
- Large technology firm was fined $466,912 for entering into an app development agreement with a sanctioned company
- “Willful violation” of OFAC by employees of a global telecommunications firm led to its $145,893 CMP
- Electronics provider to the defense industry was fined $87,507 for violating OFAC’s 50 percent rule when it dealt with an entity that was 51 percent owned by an SDN
- Technology firm fined $82,260 for providing web development services in a sanctioned country

- Software company cited for providing licenses and support services to an entity on the Sectoral Sanctions Identification List (SSI List) was fined $75,375
- Telecommunications firm fined $64,758 for its “reckless disregard for U.S. sanctions requirements by engaging in worldwide commerce without implementing even basic OFAC compliance measures”
- Software firm fined $38,930 for selling web filtering products to multiple sanctioned countries
- Data processing firm fined $23,336 for providing third-party services for a sanctioned entity

The explosive growth of the technology sector has come at a high price, including the largest OFAC fine ever imposed against a non-bank entity.

Fintechs and Electronic Payments and Trading Entities:

This industry is a first cousin to the MSB sector. In some cases, entities even fall into both categories as the rise of new digital and mobile payment systems, along with revolutionary electronic trading options, are sprouting up among a variety of industries and faster than OFAC can issue specific guidance on these entities.

To demonstrate the risk, here are a few examples:

- A well-known payments system, which processes millions of dollars in transactions on a daily basis, failed to block 486 transactions over a period of several years and was fined $7.66 million as a result. Calling its compliance program inadequate, OFAC noted in the enforcement action that the company's "management demonstrated reckless disregard for U.S. economic sanctions requirements in deciding to operate a payment system without implementing appropriate controls to prevent the system from processing transactions in apparent violation of OFAC requirements."
- An electronic trading firm, identified in its enforcement action as a small company, "failed to screen or otherwise monitor its customer base for OFAC compliance purposes at the time of the apparent violation." It suffered a $200,000 CMP
- A fintech agreed to pay $98,830 for failing to prevent persons in sanctioned areas from using its non-custodial secure digital wallet management service

Transportation and Logistics Providers:

Freight forwarders, shippers and other transportation and logistics providers play a critical role in supporting OFAC sanctions programs, as their active participation helps to block goods and vessels destined for sanctioned countries or individuals and to freeze the funds of the same. Shippers, in particular, need to note that “blocked” packages must be retained by the shipper, rather than rejected and returned to the sender.

Insufficient attention to OFAC hurt the reputation and bottom lines of these firms:

- Major shipping line fined $3.08 million for providing unlicensed shipping services to sanctioned countries
- New ownership fined $1.13 million when it discovered that the international ship management company it bought out of bankruptcy had been violating U.S. sanctions at the direction of former company leaders
- Another shipping and logistics firm fined $871,837 for failing to ascertain the complete ownership chain and interests of vessels
- Freight forwarder fined $518,063 for shipping goods through a sanctioned country
- Container company fined $374,000 for facilitating exports to a sanctioned country
- “Small” shipping company fined $157,500 for supplying fuel for a vessel from a sanctioned country

Retailers, Distributors, Suppliers and Manufacturers:

All of these industry types along the supply chain are vulnerable to OFAC violations, especially when you consider the rapid growth of international vendors in a global economy. In addition, OFAC warns that "the Internet has often been thought of as 'an anonymous venue' in that e-commerce transactions can be conducted in relative privacy with little or no face-to-face contact among the parties in a transaction. This anonymity creates a significant challenge for Internet businesses that wish to satisfy their due diligence requirements."

Retailers, in particular, need to understand whom they are selling to and whom they are receiving goods from, even those two or three steps removed on the supply chain. And manufacturers and distributors of all types of products should note that many of their peers have felt the brunt of an OFAC enforcement action, including:

- Carbon fiber manufacturer fined $7.77 million
- Chemical manufacturer fined $5.5 million
- "Small business" specializing in the manufacture of car audio and video equipment fined $4.07 million
- Metal parts manufacturer fined $2.06 million
- Tool manufacturer fined $1.87 million
- Automotive electronics distributor fined $1.5 million
- Cosmetic firm fined $996,080
- Cookware coating manufacturer fined $824,314
- Cigarette filter manufacturer fined $665,112
- Manufacturer fined $125,000 for pumps it sent to Europe that were re-exported to a sanctioned country
- Two different beverage manufacturers fined $89,775 and $27,000
- "Small, family-owned" machinery distributor fined $78,750
- "Small" international trading company fined $21,375

Expanding on its newfound tactic of sending a message to an entire industry through a particular case, OFAC has delivered multiple warnings through its enforcement actions, including this one in 2017: "This enforcement action highlights the risks for companies with retail operations that engage in international transactions, specifically including businesses that ship their products directly to customers located outside of the United States." And again in 2019, when it noted that, "This enforcement action highlights the risks for companies that do not conduct full-spectrum supply chain due diligence when sourcing products from overseas."

OFAC COMPLIANCE AND YOUR BUSINESS

In order to develop your OFAC compliance program, which should be commensurate with your organization's risk profile, you first need to understand the basics about OFAC's sanctions programs and your responsibility to them.

OFAC Sanctions Programs:

OFAC administers numerous sanctions programs, which can be divided into the following five categories. Each targets a specific type of entity or individual, blocking the property of the same and prohibiting transactions with them:

1. **Country-based:** Focused on nation states that support terrorism or the proliferation of WMDs, or undermine U.S. and international peace and stabilization efforts
2. **Country-related:** Focused on geographic areas where known terrorists, narcotics traffickers or those involved in the proliferation of WMDs are known to be located
3. **Non-proliferation:** Focused on those involved in WMDs
4. **Counterterrorism:** Focused on those identified as terrorists or terrorism supporters
5. **Counter-narcotics:** Focused on identified foreign narcotics traffickers

Transactions to Consider:

Any business transaction could potentially violate OFAC, and there is no minimum dollar amount. However, certain transactions pose a higher risk, including, but not limited to, those that are:

- Initiated from foreign countries
- Cash only, especially for large or luxury items that are easily liquidated
- International wire transfers involving international parties
- Real estate deals, especially where the borrower or seller isn't personally known
- Loan transactions, especially if the proceeds go to a third party
- With entities known to conduct business in sanctioned countries
- With a party who is anonymous or attempts to conceal their identity or location
- Where the products bought or sold change hands multiple times, especially overseas

Any business transaction could potentially violate OFAC, and there is no minimum dollar amount.

Dealing with Positive Matches:

When a potential SDN match is flagged, and additional due diligence—which is addressed in the best practices section of this paper—supports your position that it is a positive match, you must contact OFAC. If the match is significantly similar to the SDN, you need to call OFAC's hotline or use its online SDN Search Tool to help verify the match. For all exact matches and similar matches verified by OFAC, you are required to:

- Block the transaction (freeze the SDN's assets)
- Report the transaction and the block to OFAC within 10 business days via mail or email
- Refuse to do further business with the customer

CONTACTING OFAC

Office of Foreign Assets Control
US Department of the Treasury
Treasury Annex
1500 Pennsylvania Avenue, NW
Washington, DC 20220

OFAC Hotline: 800-540-6322
OFAC Compliance Division (local hotline): 202-622-2490
OFAC's Licensing Division: 202-622-2480
Email: ofac_feedback@treasury.gov

https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx

The Consequences of a Violation:

Failing to detect, ignoring, or intentionally attempting to or successfully concealing a positive SDN match leads to harsh criminal and/or civil penalties. The type and amount of the penalty depends on the sanctions program the transaction violated, any such mitigating factors as a first-time violation or a voluntary disclosure (which OFAC encourages), and any evidence of reckless or willful conduct by the violating entity. According to OFAC's website, as of April 20, 2020, the consequences for violating various programs can reach as high as the following:

- Up to $20 million in criminal penalties and 30 years in prison for willful violations of some programs
- Up to $1,503,470 in civil penalties for each violation of the Foreign Narcotics Kingpin Designation Act
- Up to $307,922 in CMPs or twice the amount of the underlying transaction for each violation of the International Emergency Powers Act
- Up to $90,743 for each violation of the Trading with the Enemy Act

SANCTIONS SCREENING BEST PRACTICES

The crux of your OFAC compliance program is its sanctions screening process. The SDN list is updated every time OFAC identifies a new individual or entity to be added or removed from that list, which often occurs daily. Your risk profile will determine how often you need to cross-check that list: with every transaction, with every new customer, or your entire customer database at periodic intervals, for instance.

With each cross-check, there is the potential for positive matches, each of which requires due diligence to confirm or rule out a match. That due diligence includes a detailed comparison of the similarities between the name, address and other information of your customer and the SDN.

Here are five critical best practices, which have been proven to significantly streamline the screening process while reducing the risk of OFAC violations and their subsequent harm.

1. **Use Outsourced List Updates:** Businesses can sign up to receive email notifications from OFAC every time the list changes, however, that equates to a manual comparison between the updated list and your transaction, customer or database. That cumbersome and inefficient method can be improved by taking advantage of outsourced list updates, where a third-party provider handles the burden of monitoring the SDN updates and provides them to you in a usable format.
2. **Automate the Screening Process:** No matter your risk profile, attempting to manually complete the screening process is just not feasible. And for businesses whose risk profiles indicate the need to screen the SDN list with considerable frequency, manual screening is both impossible and risky.

Investing in a comprehensive automated screening solution that easily integrates into your existing applications and compliance processes significantly eases your OFAC compliance burden, because it does the majority of the work for you:

- Cross-checks all of your databases against the SDN list
- Streamlines your compliance process by simultaneously cross-checking other watch lists
- Facilitates the reporting of positive matches to OFAC
- Provides detailed reports as proof of your compliance
- Decreases false positive matches by using address or date-of-birth disqualification
- Whitelists (i.e. adds to a “good customer list”) names cleared through due diligence

3. **Support Multiple Integration Methods:** Many businesses need even more support to maintain and strengthen their OFAC compliance, particularly those in the industries discussed above. The best automated screening solutions provide these additional features:
    - Facilitate and automate single SDN look-ups
    - Streamline and automate batch file runs
    - Support the review and resolve functions of multi-list screening
    - Provide enhanced search and report capabilities
    - Offer complete Customer Data Management
    - Deliver the ability to integrate into most web-based applications, onboarding systems, etc.
4. **Leverage Advanced Word-Matching Technologies:** The SDN list is full of initials, acronyms and other name variations that could result in a significant number of potential matches. This unnecessarily creates additional work for you, because it increases the amount of due diligence required to identify positive matches. For that reason, your automated screening solution must include an algorithm sophisticated enough to pinpoint true similarities and disqualify false ones. This technology reduces the number of false positives that result from your screening process, saving you time and money and allowing your staff to focus more keenly on true matches.
5. **Use an On-Demand Solution:** The final best practice is investing in an on-demand screening solution. In addition to streamlining and automating your OFAC compliance, this cloud-based type of solution puts everything—screening, searching and reporting—at your fingertips anytime and anywhere you need it through the use of secure credentials.

GAIN COMPLIANCE AND EFFICIENCY THROUGH EXPERTISE AND AUTOMATION

OFAC compliance is complicated but the cost of non-compliance is too steep to risk it. The only viable solution is incorporating many or all of the best practices outlined in this white paper, depending on the size, type and risk profile of your business. These proven methods provide both compliance and cost efficiency, because they are developed by regulatory experts and are delivered through sophisticated automation techniques.

ABOUT CSI

Computer Services, Inc. (CSI) delivers innovative financial technology and regulatory compliance solutions to financial institutions and corporate customers across the nation. CSI's advanced compliance software solutions employ the latest technology to automate and streamline sanctions screening, filing and fraud prevention, while minimizing false positives and reducing labor costs. Our comprehensive compliance testing, auditing and training services strengthen your practices and protocols in the face of rapid regulatory change and improve risk management to protect the integrity of your business. For more information about CSI, visit csiweb.com.