DESCARTES™
Visual Compliance

EXPORT COMPLIANCE WHITE PAPER

Clarifying Restricted Party Screening Misconceptions

2019

Table of Contents

Compliance and screening-related misconceptions, resulting in fines and other penalties—don't let them happen to you

Why organizations need to screen against Restricted and Denied Parties Lists

Screening for restricted and denied parties, as well as helping to ensure that goods, technologies, or services are not destined for a sanctioned or embargoed country—not to mention screening every financial transaction—should be an integral component to every organization's governance, risk and compliance objectives.

While homeland security-sensitive industries, such as aerospace and defense, telecommunications, information technology, energy, research and financial institutions, have a high bar when it comes to complying with U.S. and international export, trade and financial laws, the fact is that all businesses have an obligation to adhere to compliance requirements.

Companies found in violation of international trade regulations come from across all industries—in fact many organizations that have received financial, or even criminal penalties, fall outside the realm of the higher-risk industries noted above.

In this document, we have highlighted a seed distributor, a car leasing business, a passion fruit buyer and a travel agency, among others, to underline the point that ordinary businesses can also fall foul of the law.

But many companies, both large and small, often neglect this important aspect of their compliance program because of the misconception about their level of risk, believing that their business and industry is somehow exempt. Or that to be export, trade and OFAC compliant has to be an onerous task, or one that comes at great expense.

In most instances, neither is the case.

Within these pages, we have listed the top misconceptions we've heard in our close-to-40-years in the industry with regards to why a company does not screen. We've also included relevant examples of actual export violations—and the penalties thereof—to demonstrate the real-world consequences of non-compliance.

Our aim is to give organizations considering abandoning the practice of Restricted Party screening, or not adopting altogether, some food for thought.

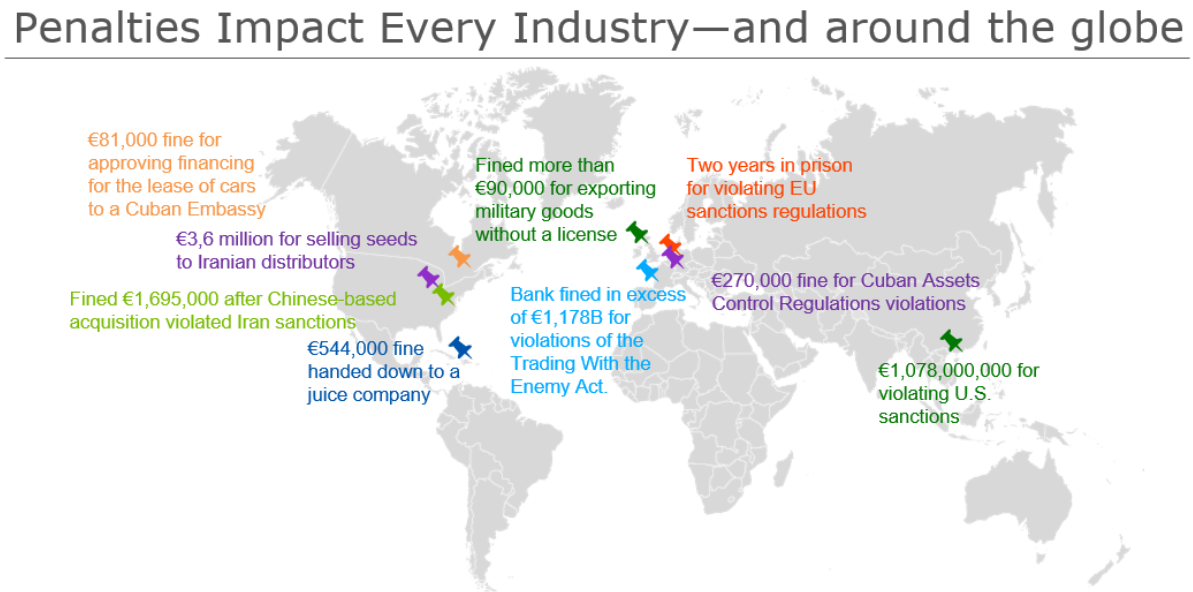
"We don't need to screen"—11 myths that might surprise you

Myth 1—it doesn't apply to our business, industry, or country

All businesses have an obligation to be screening against denied parties not just those in homeland security sensitive industries. This includes businesses not based in the U.S. as well. For as long as an organization engages with the U.S. in any capacity—including selling products and services in the U.S., or even using U.S. banks and financial services for transactions—they are subject to U.S. export and financial compliance laws.

Consider the following examples, demonstrating the geographic width and breadth of industries that are subject to U.S. export laws:

- In 2016, a juice company was found in violation of the Narcotics Trafficking Sanctions Regulations when they purchased passion fruit juice/pulp from an organization on OFAC's SDN list. The **base penalty for the violations was €544,000**.
- In 2016, a Seed Company was **fined over €3,625,000** for selling flower seeds to distributors in Iran. While this violation was committed by the company willfully, that the sale of flower seeds could result in such a large penalty dispels the notion that only certain industries are subject to export or OFAC violations.
- In 2018, a French bank was **fined €1,178,000,000** for violating the Trading with the Enemy Act by processing transactions worth billions of dollars for Cuban banks.
- In 2019, an Australian national was **sentenced to 2 years in prison** for exporting electronics to Iran, and extradited to the United States to carry out his sentence.



Myth 2—we only supply services, so we don't need to screen

Every time money changes hand, there is an obligation to ensure that the good or service is not destined for an individual or entity on a government watch list. There's also a misconception that this only applies to financial institutions, but take the examples below from the auto financing, and travel and tourism industries, respectively:

• In 2019, a leading online travel agency received a fine of over €270,000 for violating the Cuban Assets Control Regulations (CACR) by enabling 2,221 people to travel within, or to and from, Cuba.

• An auto financing company was fined close to **€81,000** in 2017, by way of its Canadian subsidiary, for approving financing for the lease of cars to the Ottawa-based Cuban Embassy.

• In 2015, a travel company was fined €39,800 for providing Cuba-related travel related services.

Myth 3—We rely on a third-party, such as our customer or freight forwarder, to do our screening for us

It's a common misconception that the burden of compliance rests with the shipping or forwarding company, tasked with ensuring the goods get to their destination. This is not always the case, as the U.S. government can designate the owner or seller of the merchandise being exported (or imported) as the Exporter of Record. Meaning that the onus of compliance falls on both organizations.

Freight forwarders themselves aren't immune to export violations, as the examples here, here and here demonstrate.

Myth 4—We don't export outside the U.S.

A significant number of those found on watch lists are U.S. nationals or citizens located in the United States who have been found guilty of violating export laws. Meaning that even though someone is located in the U.S.—or on any organization's home soil, for that matter—there is still an obligation to screen regardless of destination. For example:

- Two Washington State men were placed on **the Department of State's Debarred list** after being convicted of illegally exporting controlled goods in 2009 and ordered to pay close to €81,000 in criminal fines.
- A Maryland man was placed on **two separate government watch lists** after being sentenced to five months in prison in 2011 for attempting to illegally export firearms and ammunition without the required licenses.

Myth 5—We're located outside the U.S.—export laws don't apply to us

Regardless of where in the world an organization is based—be it their global headquarters, or subsidiaries thereof—odds are at least some, if not all, transactions flow through the U.S. financial system at one point or another in the purchasing or supply chain process. As such, these transactions inherently fall under the purview of the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC).

And should they involve restricted or denied individuals or entities, or sending unlicensed controlled goods to sanctioned or embargoed countries, they can result in stiff penalties.

Moreover, **European and other global regulatory bodies have their own sanctions programs in place**. This means that with few exceptions, all organizations, regardless of industry and geography, should have export, trade and financial compliance measures in place.

Consider the following:

- In 2017, a Singapore-based technology company was fined over €10,900,000 for doing business with Iranian entities via a US financial institution.
- 304 violations of the Cuban Assets Control Regulations by a German subsidiary of a U.S. company resulted in a **monetary penalty of over €4,540,000**.
- The UK has issued multiple fines in recent years to individuals and organizations unlawfully selling goods requiring export licenses. In one notable case, the goods themselves did not originate from the UK, but did involve a UK national.

Myth 6— We don't export to countries under sanctions or embargoes

Virtually every nation, on every continent (yes, even Antarctica) has debarred individuals and entities inside their borders. Ranging from dozens to hundreds, it means that regardless of where in the world an organization exports to—or with whom they transact internationally—they run the risk of engaging with a denied or restricted person or organization.

Myth 7—Our goods are EAR99, so we don't need to screen

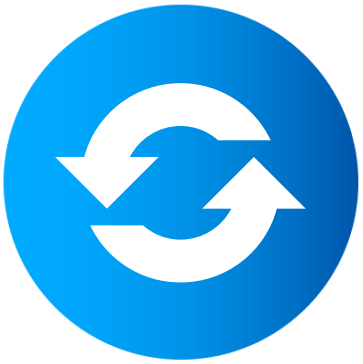
An organization's goods might be EAR99, however, selling them to a denied party is still illegal. Only by screening every individual or entity, regardless of whether the product or technology is controlled, will an organization be in compliance with U.S. trade, export and OFAC laws and regulations.

The 2017 edition of the Bureau of Industry and Security's *Don't Let This Happen to You* is replete with examples of EAR99 export violations.

Myth 8—We already screened our customers and contacts once

Just because a business or individual isn't on a government watch list today, yesterday, or even three weeks or three months ago, doesn't mean that an organization will lawfully be able to do business with them tomorrow, or in a week, months or years to come. Or vice versa—on a list today, and off tomorrow. This is primarily due to the frequency in which denied and restricted party watch lists change—in many cases daily. With that in mind, organizations would be best served by screening all transactions, and at multiple times throughout the business workflow.

For example:



- Thousands of organizations from across the globe had long-standing business dealings with Zhongxing Telecommunication Equipment Corporation (ZTE), which is facing over €908,580,000 in financial penalties from multiple government agencies for a series of Iran sanctions violations dating between 2010 and 2016**. While under sanctions for a relatively short period of time, it was still unlawful for those organizations to transact with ZTE during that time.** However, mitigating factors eventually saw the ban lifted, and they're currently in the clear (although some ZTE-related entities that played intermediary roles remain on U.S. government watch lists).

It's worth noting that "screening all transactions" should also include checking the destination country against sanctions and embargoes, suppliers, vendors, visitors—in fact, an organization will never go wrong if they screen every person or entity that falls into their sphere of business.

Myth 9—The person who screened has left the organization

The legal requirements behind having export, trade and OFAC compliance processes in the first place will rarely—if ever—change. It is therefore crucial that the primary compliance champion passes the baton to a successor to keep the work moving forward. Even more sensible is to **instill a culture of compliance across the entire organization.**

In 2018, the Bureau of Industry and Security (BIS) handed out €908,580,000 in fines. That same year, OFAC levied over €1,090,155,000 in monetary penalties.

Myth 10—The project for which we needed to screen is complete

It's not just about what an organization manufactures and then sells, or which research projects may be currently underway. This is especially the case if organizations deal in controlled technologies, aka, deemed exports—in particular, those who have access to said technologies.

- A tool manufacturer committed multiple export violations between 2003 and 2007, resulting in a fine of €114,300. Chief among the violations was the release of controlled technology to Italian and Indian nationals employed by the company without the required licenses.

Myth 11—We'll just pay the fine if it comes to it

Fines that come as result of an export or OFAC violation should not be treated as a business expense. In fact, criminal penalties can also include jail time, and organizations can even have their export privileges denied—neither of which are ideal for any company wishing to remain a going concern.

Moreover, negative—or adverse—media attention is an increasing concern for risk-averse organizations who want to protect their own reputation by avoiding business with non-law-abiding people or companies. With export and OFAC violations information readily available online, and with more companies upping their GRC efforts and proactively looking at negative news, getting slapped with a fine is just one piece in the proverbial penalty pie, as the example below shows:

- In 2017, a former managing director of a Dutch company was sentenced to almost two years of imprisonment, after being found to be in violation of EU sanction regulations.

Myth 12—We only need to screen the person to whom we are shipping

One of the most misunderstood areas of export compliance is that of the requirements surrounding end use. Not to be confused with the purchaser, or country of destination on record, end use compliance goes one step further by requesting documentation from the purchaser that they are, in fact, the ultimate destination of the good or product. And that they will use the good or product as intended. This is typically done by asking for an end user statement that is then kept on file for recordkeeping purposes.

While obtaining an end user statement doesn't guarantee that the person on the other end is being 100% truthful, its importance lies in demonstrating that an organization has taken additional measures to help ensure they are putting in their best efforts to adhere to export and trade compliance laws.

In an example announced in 2019, a US-based maker of atomic clocks was not handed a fine after red flags had them go above and behind their end use compliance, going so far as to demand a site visit to the purchaser. Said export violator is still at large, but had they not gone to such exacting lengths, they could have received a fine of upwards of €908,400 and even decades of prison time.

Descartes Visual Compliance™ has a full suite of restricted party screening solutions to help navigate the ever-changing, complex world of trade compliance

Descartes Visual Compliance™ offers advanced restricted party screening solutions that are used by companies around the world to comply with international trade regulations, and to significantly reduce the risk of negative impacts to reputation and the bottom line.

Descartes Visual Compliance Restricted Party Screening solutions are affordable and modular, giving organizations the ability to get up-and-running quickly, and add supplementary solutions should requirements change in future.

Whether an organization needs to screen on an ad hoc basis, or is looking for automated solutions to fit into existing business systems (ERPs, CRMs, etc.), we have solutions that can help meet screening obligations with ease, efficiency, and unmatched reliability.

Key takeaways

Ultimately, any export, trade and OFAC compliance violation that result in penalties could affect a company's bottom line. And in the worst-case-case scenario, sound the death knell to the business. To help prevent this from happening, having a restricted and denied parties, and sanctioned and embargoed countries screening program in place is critical.

But organizations that take compliance seriously go even further by embedding a culture of compliance that works in tandem with compliance software. Having an internal Champion (or even Champions) of Compliance will not only help ensure that screening is taking place as it should, but in the event of an accidental violation, will be seen as a huge mitigating factor in helping to lessen the response from authorities—and may even prevent penalties from happening altogether.