Steps For Companies New To Sanctions Compliance

By **Jennifer Schubert and Megan Church** (February 26, 2024, 6:02 PM EST)


Jennifer Schubert


Megan Cunniff Church

Is the U.S. at war with business? It may seem that way to some international market participants.

In response to global threats, the U.S. government has flexed its vast economic muscle, using unprecedented and expansive sanctions and export controls to keep international aggressors unarmed and short-handed — with newly regulated businesses at risk of becoming collateral damage if unprepared.

To add insult to injury, businesses must also be mindful of sanctions-evasion tactics by those attempting to circumvent compliance systems — including intermediary fraud.

How can businesses fight back? Guidance on the best practices for navigating this minefield is distilled below for companies and their counsel alike.

Global Enforcement of Economic Controls in New Industries

With 2023 in the rearview mirror, it has become clear that the U.S., in its efforts to combat Hamas and Russia, has taken its economic controls far beyond traditional military-related sanctions.

That vantage was reinforced last week, following the death of Russian opposition leader Alexei Navalny, with **the** announcement of the largest round of U.S. sanctions against Russia since it invaded Ukraine two years ago.

It is crystalline that U.S. sanctions and export controls now pervade the aerospace, maritime and energy sectors, with impacts on financial institutions and financial technology companies, engineering, electronics and robotics, metals and mining, construction, manufacturing, seafood, and luxury goods — as well as the provision of all unregistered services to sanctioned entities.

The U.S. previously also announced sweeping economic controls geared at halting Chinese development and market domination, largely affecting the technology sector, including semiconductors, biotechnology and artificial intelligence, among others.

What is more, stronger U.S. regulatory enforcement programs, increased prosecutions and heightened penalties for violators go fist in glove with the ever-growing lists of sanctioned individuals and controlled products.

The U.S. Department of Justice and other enforcement agencies have announced their heightened expectations of industry compliance, remediation and voluntary self-disclosure of wrongdoing. Such compliance efforts are necessary to mitigate — or can aggravate, when lacking — prosecutions and regulatory enforcement outcomes, including deferred or nonprosecution agreements and fines.

The U.S. is not alone in its expansion of sanctions into less traditional industries with accompanying enforcement efforts.

International participants at the London Forum for Global Economic Sanctions in late fall 2023 discussed how the Export Enforcement Five — consisting of Australia, Canada, New Zealand, the U.K. and the U.S. — also announced restrictions, not only on direct use, but also on dual-use components of military supplies.

And in its 11th and 12th packages of sanctions against Russia, the European Union announced a ban on provision of intellectual property or trade secrets to Russia, as well as export restrictions on luxury vehicles, chemicals, thermostats, certain motors and machinery, and diamonds, including lab-grown diamonds and jewelry containing diamonds.

In forceful synchrony with the latest U.S. sanctions, on Feb. 23, the EU adopted its 13th package of sanctions against Russia, bringing its designation list to over 2,000 individuals and entities. This package specifically targets Russian acquisition of aerial vehicles, and drones and their component parts, aiming to ground Russia's drone warfare.

Evasion and Intermediary Fraud

As the lists of sanctions grow, the list of lawful end-consumers dwindles. And with increased enforcement comes increased evasion tactics, and more sophisticated attempts to bypass sanctions.

Businesses must be vigilant. What at first blush may appear to be a valid consumer may in fact be an intermediary that is servicing a sanctioned end-user.

Alina Nedea, head of sanctions for the European Commission, noted at the forum last fall that unsanctioned countries and profiteers have found a positively lucrative business in setting up shell entities to purchase dual-use, sanctioned goods, and resell them to sanctioned end-users.

Relatedly, the European Commission identified suspicious trade patterns that confirm this conclusion: new trade between European countries and third-party countries where such flows previously did not exist, spikes in product purchases outside the purchaser's usual market, and correlative trends of that product being exported quickly after the abnormal purchase.

The Feb. 23 sanctions aim to cut these evasion patterns off at the pass. President Joe Biden underscored that the new U.S. sanctions target those "providing backdoor support for Russia's war machine."

The U.S. Department of the Treasury and the U.S. Department of State echoed this in their respective press releases.

The Treasury similarly declared its designation of "more than two dozen third-country sanctions evaders" spanning Europe, East Asia, Central Asia and the Middle East. The State Department highlighted sanctions imposed against those engaged in "evasion and circumvention."

The message is clear: Intermediary fraud will be treated as direct support of Russia's war on Ukraine and punished accordingly.

Compliance Guidance

In all, the sanctions landscape heightens the burden and potential cost of operating in international markets. While companies in certain military-focused industries, like arms manufacturers, and steel- and military-equipment providers, have traditionally faced intense regulation, manufacturers of dual-use goods and luxury products, as well as the transportation industry and other service providers, are in less familiar territory when confronting the effects of sanctions and export controls.

Sanctions and export controls exercised by the U.S., the EU and European countries are pervasive and not all in sync, creating a minefield of restrictions that businesses in the international marketplace must navigate.

Newly affected industries may lack robust compliance programs and be more vulnerable to intermediary fraud. And if they misstep, they may become the targets of criminal prosecutions or other enforcement actions.

International market participants — particularly in these newly regulated fields — and their legal counsel must exercise vigilance, and be aware of the ribbon of sanctions and export controls that runs through their business interests.

Regulators have strongly advised those engaged in myriad affected industries to implement proper compliance measures to reduce their risk of falling victim to fraud or becoming the subject of prosecution.

They have also offered lawful actors high-level guidance to help them avoid collateral damage in this economic battlefield.

Robust Compliance Programs

For years, U.S. prosecutors and regulators have warned businesses in highly regulated industries and global markets to implement effective compliance programs designed to detect and remediate misconduct that violates U.S. law and regulation — or suffer significant legal and financial consequences when they fall short.

Through a recent tri-seal compliance note and subsequent guidance, the DOJ, the U.S. Department of Commerce and the Treasury emphasized the fundamental importance of having "an effective and sufficiently resourced compliance and ethics program."

The Office of Foreign Assets Control has also indicated that, when a company is under investigation for a potential sanctions violation, it expects to see specific elements in its compliance program. And EU regulators have noted that they look to the OFAC guidance as a source of best practices across industries.

Broadly speaking, U.S. agencies and regulators agree that businesses with existing compliance programs must ensure that those programs are robust, current and can actively detect wrongdoing. A compliance program cannot be rote or perfunctory; rather, it should be meaningful and effective.

For new businesses or businesses encountering new regulations, it may be necessary to set up a data review and compliance program. It can be a huge lift to start a compliance or screening program.

Such companies need to find vendors, choose and implement screening systems, evaluate and determine their risk tolerance, set corresponding risk parameters and date ranges, and assess which parts of their business to screen.

At the forum, OFAC laid out its five essential components of sanctions compliance.

1. Senior Management Leadership and Buy-In

Senior management at the company must review compliance policies and procedures, understand how compliance operates within the company and create "cultural compliance." In other words, compliance should not be delegated, but should start at the top, and be encouraged and employed at every level.

2. Intentional Risk Assessment

While efficiencies may dictate that not every single product or area of business can or should be screened, businesses taking a risk-based approach should do so based on meaningful determinations about their risk.

For example, a cellphone company that also produces cellphone novelty cases might decide not to screen customers purchasing only cellphone cases. That screening decision should be based on reasoned conclusions — e.g., cellphone cases are not a controlled product and are unlikely to raise sanctions risk.

After making that decision, the cellphone company may then decide not to put controls in place for that product line, saving time and money.

The cellphone company might then focus its compliance efforts on its technology products, treating those with measurable attention.

If, later, an issue arises from its cellphone case sales, the company could defer to the policy in place and justify its risk assessment decision.

Businesses may also rely on other market-based considerations when assessing risk. Hong Kong, Turkey, Cyprus and the United Arab Emirates are widely known to circumvent sanctions.

Companies should consider extra screening for customers from those countries of origin, and potentially use less rigorous screening for countries with whom they have had lawful, historic working relationships.

In short, risk assessments can be done in different ways, but there should be a reasoned, intentional assessment of risk at the foundation of a screening program.

3. Internal Controls

Businesses should adopt formal and clear policies, procedures and systems, with tiers of review for data and information. Strong compliance programs should include continual, systematic review of international sanctions lists and revised export control lists.

This may include running checks on product codes to see if they are newly subject to controls, as well as screening business partners, end-users and other transaction participants to see if they are newly

subject to sanctions.

Additionally, September 2023 guidance from the Bureau of Industry and Security recommends that for transactions involving the highest priority listed items, companies should "seek written assurances of compliance from their customers to help prevent diversion."

Compliance programs should detect suspicious activity beyond the obvious red flags. OFAC has indicated that important data should be reviewed, including detailed line-by-line information about the parties to a transaction.

A business can rely in part on technological tools to review party phone numbers, nationalities, passport data, email, and IP address origins or other geolocation information. The data may either corroborate or contradict a party's representations about their identity or location, and may raise red flags that need to be addressed.

For example, if a party represents that they are from a nonsanctioned country of origin but has an IP address or phone number country code associated with a sanctioned country, this contradiction should raise a red flag and instigate further review.

OFAC also noted at the forum that businesses must use constant vigilance. They should conduct data review, not just at the outset of a relationship, but at intervals over the course of an extended relationship to address the potential for changed information.

Likewise, when a business develops or transacts in a new product line or industry, they must be added to its screening and controls. New business partners, vendors and customers must be included as well.

4. Testing and Auditing

Having a compliance system and clear policies and making risk assessments are not enough. Businesses should conduct periodic testing and audits to check if their compliance measures are working properly.

Simply collecting the information is not enough — it must be correctly analyzed and then used. This is a constant work in progress. If issues or holes are identified through testing and auditing, they should be corrected and retested.

5. Training

Finally, OFAC encourages businesses to conduct formal training that ensures their different components understand the compliance systems, and their respective roles in enforcing compliance.

Employees responsible for any part of the business's compliance system should understand the tools being used, how to review the data and what constitutes a red flag. Businesses should also educate those employees about evasion tactics and how to detect them.

For example, employees should understand how to watch for specific changes in data, such as sudden spikes in order volume by Russian or Chinese allies, changes in product sale patterns, or new and unusual customer purchase patterns.

Employees should also understand procedures for handling and swiftly escalating red flags within the

business organization.

Conduct Internal Investigations Early

Businesses and their legal counsel must be prepared to swiftly undertake remedial action when red flags arise, and to investigate problem areas. It may be enough if the business evaluates and corrects its compliance systems and tools, but more digging may be required to get to the bottom of a larger problem.

If there is an indication of a more substantial issue, businesses need to be ready to assess the scope and nature of the problem quickly and thoroughly. As the BIS recommends, businesses should work to improve compliance systems, strengthen remediation and identify the best next steps to prevent future issues.

Consider Voluntary Self-Disclosure.

At the New York City Bar's International White Collar Symposium last fall, Associate Deputy Attorney General Marshall Miller underscored the messages of the tri-seal compliance note on voluntary self disclosure of potential violations, previously issued by the DOJ, the BIS and OFAC.

Miller expressed hope that the voluntary self-disclosure policy will result in more corporate whistleblowing. The DOJ's National Security Division and the U.S. Securities and Exchange Commission, among others, also take into account self-disclosure when evaluating outcomes for businesses and individuals under investigation for violations of U.S. laws and regulations.

Many considerations are at play when deciding whether to self-disclose. Is there really a violation? Is the violation reportable? When should we disclose? How much information do we need to have before disclosing it? How should we disclose? And where — to the DOJ or to a regulator?

Conclusion

The sanctions and export control landscape is perilous and ever-evolving. Businesses operating in international markets and affected industries can still thrive and avoid becoming collateral damage in the economic battles being waged against international aggressors and adversarial markets. By implementing effective compliance programs, businesses can ensure that they remain on the right side of enforcement.

Jennifer Schubert and Megan Cunniff Church are partners at MoloLamken LLP.