

Sanctions Compliance Tips For A Dynamic Global Landscape

By **Kenneth Feinstein, Robert Brunner and Daniel Castleman**

(April 27, 2020, 7:24 PM EDT)

The corporate compliance landscape has shifted considerably in recent years, highlighted by the de facto deregulation of white collar crime juxtaposed against the increased focus on global trade. Necessarily, the ongoing COVID-19 pandemic[1] has once again shifted the landscape. Regulators and corporate executives are temporarily shifting their focus to the health, safety and economic impacts of the coordinated global response.

Regardless, as increasingly scarce resources are redirected toward mitigating short-term needs and risks, companies are nonetheless continuously challenged to identify, manage and monitor compliance risk to avoid potential violations. Other than considering an easing of sanctions to alleviate humanitarian concerns, there is no evidence that regulators have curbed their aggressive pursuit of compliance imperatives. All industries need to maintain vigilance while evolving their global business practices.

Regulatory Environment

With the growing risks of sanctions and trade regulation noncompliance, in addition to reduced or reallocated compliance funding due to financial hardship, companies will be expected to continually evaluate and recalibrate their strategies. Prior to the spread of COVID-19, compliance programs were transforming to support strategic goals and regulatory exposure.

The U.S. Department of the Treasury Office of Foreign Assets Control, or OFAC, administers and enforces economic and trade sanctions programs to support U.S. national security goals and foreign policy objectives. Sanctions programs[2] target governments, regimes, entities and individuals with interests that run contrary to those of the sanctioning government.

The current regulatory environment, saddled with the additional weight of disruption caused by a growing pandemic, could increase a company's exposure to trade sanctions. Among other impacts, violations could have a destructive impact on a company's reputation and ability to engage with third parties on a global scale, and/or give rise to substantial penalties. Effective monitoring programs can



Kenneth
Feinstein



Robert
Brunner



Daniel
Castleman

directly reduce the likelihood of these consequences.

Regulators, including the U.S. Financial Crimes Enforcement Network, the U.S. Department of Justice, the U.S. Office of the Comptroller of the Currency, or OCC, and others, have issued additional guidance related to the ongoing pandemic.

On April 20, OFAC released guidance[3] that supports a risk-based approach to sanctions compliance. According to the recent action, OFAC will evaluate technical and resource challenges caused by COVID-19 as a factor in determining the appropriate administrative response to an apparent violation that occurs during this period.

Recent Enforcement Actions

According to the Department of Treasury, since the start of 2017 there have been 47 OFAC enforcement penalties totaling over \$1.4 billion.[4] Recent settlements include:

- In January, Eagle Shipping International LLC settled a \$1.1 million civil liability for multiple violations of the Burmese Sanctions Regulations, involving dealings with an entity identified on OFAC's specially designated nationals and blocked persons, or SDN, list. It was the first such settlement in 2020 and highlights growing risks in the logistics industry.
- Standard Chartered Bank was fined \$640 million in April 2019 for violating the Cuban embargo and Iranian, Syrian, Burmese and Sudanese sanctions. This institution processed thousands of transactions through the U.S.
- In March 2019, Stanley Black & Decker Inc. was fined \$1.86 million by OFAC for 23 violations of Iranian sanctions involving the direct and indirect export of millions of dollars of goods to Iran. OFAC used the case to outline what a comprehensive compliance program is expected to include.

Risk Exposure: Weighing Prudence Against Necessity

How does one weigh prudence against necessity? The answer differs by industry, company and even person, but one thing is certain: Compliance is not postponed due to a virus outbreak.

When the economy recovers, prosecutors and regulators will be holding companies accountable for behavior before, during and after the crisis. For now, compliance departments must effectively and efficiently allocate resources to mitigate risk even during these turbulent times.

Compliance officers overseeing international trade should be thinking about how to avoid violating sanctions by developing an effective compliance program based on authoritative guidance, leading practices and their organization's unique facts and circumstances.

Easier said than done? Not necessarily, especially if the program is broken down into realistic steps and a reasonable timetable is set for implementation and adoption.

Authoritative guidance — best left to the regulators and not management — should be the foundation on which a program is built. OFAC has provided a framework[5] for management teams to follow as they design and implement compliance activities across organizations.

The straightforward guidance, updated to reflect OFAC's most recent action regarding COVID-19, focuses on key fundamentals, including board oversight management responsibility, compliance risk assessment and monitoring, and internal controls.

The concept of leading practices is subjective, and varies depending on the source and timing of their dissemination. Dynamic geopolitical influences can, and do, have a significant impact on what legal and compliance advisers consider to be the practice du jour.

Similarly, whatever authorities and leading practices dictate, such guidelines should be reconciled to the risks identified from the company's internal assessments. Ultimately, in addition to a well-designed compliance framework and a good-faith implementation, the Department of Justice expects a program that works.[6]

To that end, it is important to emphasize monitoring, the proactive efforts put in place to reduce the risk of costly reactive matters. This is particularly relevant in the shadows of a global crisis where the lack of watchful eyes could create a breeding ground for fraud, corruption and noncompliance.

An integrated compliance monitoring program requires involvement from the business process owners, access to data from accounting and operations systems, and professionals who understand the technology and supply chain process.

Forensic analysis helps identify transactions that are potentially problematic, i.e., OFAC violations, because they may involve prohibited product shipments or supplier payments to prohibited third parties through the U.S. financial system. Subsequent findings can then be retroactively applied to a company's data in order to identify potential gaps in historic compliance monitoring, inform the filing of voluntary self-disclosure reports with regulators and mitigate penalties.

Investigative Data Analytics

Considering the vast landscape of systems that companies employ, including finance, accounting, operations, purchasing, logistics and sales, and the high volume of transactions that flow through these systems, it can be nearly impossible to pinpoint which activity poses the most significant threat to an organization. Analyzing data from these sources is most effective when the search targets are known — but is that a reasonable expectation?

An investigative data analytics approach combines structured and unstructured[7] data analytics with traditional investigative methodologies to flag potentially violative transactions and problematic third parties.

An effective analytics-driven plan can isolate specific transactions, including shipments of goods or services provided to customers in sanctioned jurisdictions, payments made to vendors on OFAC's SDN list or funds issued from sanctioned entities through U.S. banks. Once the profile of such business activity can be identified within the data, it's much easier to construct a program to concurrently analyze multiple data sources in search of transactions exhibiting a similar pattern.

Analytics performed in isolation can be ineffective, to say the least, and prove to be costly; red herrings abound. Value can be gained from having results interpreted by qualified individuals.

Safeguarding Organizational Identity

In the wake of economic crises, legal and compliance departments scramble to address new and changing issues. Risks emerge and evolve, technology improves (e.g. social media analytics, communication tools), and unforeseen shifts occur in the global economy (e.g. fallout from COVID-19). The one thing that won't change is the importance of an organization's identity, which demands a commitment from leadership and support from employees.

Commitment requires more than a town-hall meeting, newsletter, email or even a tweet. It requires investment in people and technology; providing employees and advisers with the funds, tools and flexibility to inspire process innovation in a safe yet collaborative environment.

This can be achieved through readily accessible training materials, consistent and reinforced internal and external communication, and incentive programs that keep employees engaged and focused on the company's strategic vision.

Whether a company produces widgets, provides services, sells goods or accommodates travel and leisure activities, no industry is safe from the unexpected. In just the last two decades the world has experienced several jarring events that directly impacted billions and changed our way of life.

The attacks on Sept. 11, 2001, challenged the resiliency of our national security and forever changed how we travel and the 2008 financial crisis shook the foundation of our economy and paved the way for stricter oversight that helped shape the financial services regulatory environment. The outcome of the ongoing coronavirus pandemic is yet to be determined, but companies that promote a culture of integrity, accountability and transparent communication will be better positioned to prevail and sustain success as landscapes continue to change.

Kenneth Feinstein is a principal, and Robert Brunner and Daniel Castleman are vice presidents at Charles River Associates.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] World Health Organization, Coronavirus disease (COVID-19) Pandemic, <https://www.who.int/emergencies/diseases/novel-coronavirus-2019>.

[2] Countrywide sanctions programs include Iran, Syria, North Korea, Cuba, the Crimea region of Ukraine, and other specially designated nationals and blocked persons that include entities and individuals.

[3] U.S. Department of the Treasury, Resource Center, The Office of Foreign Assets Control (OFAC) Encourages Persons to Communicate OFAC Compliance Concerns Related to the Coronavirus Disease 2019 (COVID-19), April 20, 2020; <https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20200420.aspx>.

[4] U.S. Department of the Treasury, Resource Center, <https://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx>.

[5] U.S. Department of the Treasury, “A Framework for OFAC Compliance Commitments,” https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf.

[6] U.S. Department of Justice, Criminal Division, “Evaluation of Corporate Compliance Programs,” April 2019, <https://www.justice.gov/criminal-fraud/page/file/937501/download>.

[7] According to Datamation, structured data is comprised of clearly defined data types whose pattern makes them easily searchable; while unstructured data — “everything else” — is comprised of data that is usually not as easily searchable, including formats like audio, video, e-mail, chat sessions and social media postings.