GAN INTEGRITY

Accounting for third party risk: a framework

The most critical component of an effective third party risk management ("TPRM") program is proactive identification of tangible risk factors based on actual lessons learned by the company both internally (as a consequence of its own practices) and externally (as a result of industry-specific regulatory changes and enforcement actions). As regulatory and enforcement agency guidelines repeatedly emphasize, a company's TPRM practices must be subject to continuous evolution and improvement. This makes periodically revisiting an organization's TPRM profile an imperative in a climate prone to frequent changes in the state of applicable law

Mere identification of such risk factors in isolation, however, is insufficient to meet an organization's core TPRM responsibilities. To ensure that emerging risk factors are effectively addressed, the organization must integrate those factors into its overall TPRM profile—ensuring that the company holistically adopts internal controls designed specifically to reduce the likelihood that a particular third party could expose the organization to considerable legal or regulatory risk.

Even more importantly, the adjustment of the organization's TPRM profile should be accompanied by changes to its enterprise-wide risk assessment, especially in cases where such changes affect the overall prioritization of other competing risks. The failure of the organization to properly account for third party risk within the broader framework of an enterprise-wide risk assessment is a recipe for disaster.

> **"Companies that lack visibility into the complete universe of concrete risks are unable to effectively address those risks by prioritizing appropriate mitigation and resource allocation efforts."**

While third parties will typically present significant risks regardless of industry, these challenges can vary widely between different types of businesses. While off-the-shelf compliance products may be helpful, most high-risk, highly regulated industries can benefit greatly from tailored compliance tools that can be customized to the specific risks inherent in the business. The right provider can even help companies look beyond the horizon and identify key challenges in the near future and—most importantly—prepare a company to be ready to address them before they create any liabilities. In that vein, we examine some of the greatest challenges faced by several key industries in the current regulatory environment.

Oil and gas industry

The oil and gas industry has become fraught with risks, which only seem to multiply as time elapses. Considering oil and gas tends to be a key source of revenue for many governments, it is no surprise that these wealth drivers are targeted by various trade sanction and export control programs. Look no further than the complex web of sanctions imposed on the Russian Federation following its invasion of Ukraine. Up until that point, entities operating in the oil and gas industry were already navigating complex terrain. Several prominent companies in the Russian oil industry, such as Rosneft Oil Company, have been subject to sectoral sanctions since 2014, which prohibited U.S. companies from participating in certain specified projects with these entities, such as projects related to deepwater drilling, Arctic offshore drilling, and shale oil projects.

More recently, however, the Biden Administration has ramped up these restrictions in an attempt to cripple Russia's economy. For one, President Biden issued an Executive Order that banned the import of Russian oil, liquefied natural gas, and coal to the United States. This places a heavy burden on companies operating in this industry, as they must be sure that the various petroleum products they seek to import to the U.S. are not of Russian-origin.

Furthermore, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") added several new oil and gas companies to its Specially Designated Nationals and Blocked Persons ("SDN List"). Additionally, several key Russia oligarchs and businessmen have been added to the SDN List, which, according to OFAC's 50 Percent Rule, also effectively prohibits U.S. persons from transactions with any of the myriad of companies of which these individuals hold the majority of ownership. And these are just the U.S.'s regulations; many other western allies have implemented their own sanctions impacting the oil and gas industry. While many align closely with the U.S., several have their own unique nuances that companies need to be aware of.

These prohibitions implicate a multitude of complex issues. As previously mentioned, the Russian oil and gas industry has been subject to some level of sanctions for several years now. Prohibited parties continue to learn and develop new methods to attempt to circumvent these sanctions. Sanctioned Russian entities are well known for employing a variety of schemes designed to hide, obfuscate, and deflect potential sanctions risks, such as utilizing shell companies to hide ownership by sanctioned oligarchs.

OFAC sanctions are a strict liability offense, and such actions by sanctioned parties will not necessarily preclude OFAC from pursuing charges against companies that unintentionally engaged with a prohibited party.

> **"Companies operating in the oil and gas industry must be sure to obtain complete beneficial ownership information of the parties they transact with, conduct comprehensive due diligence, and properly analyze any risks that may appear in the review"**

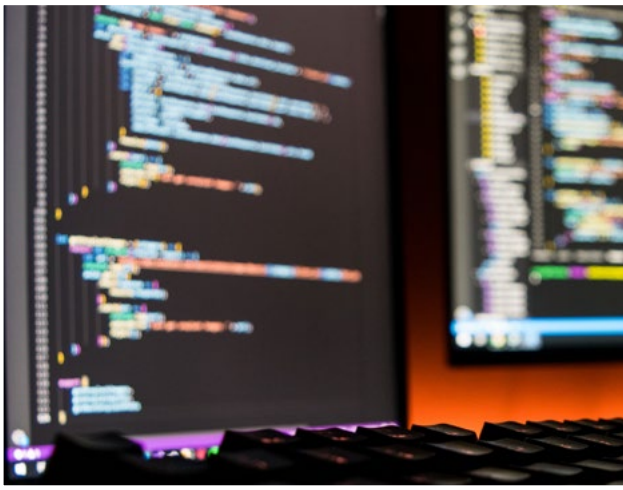
We expect these risks to continue to increase in the foreseeable future. For one, it does not appear that the sanctions on Russia are likely to be lifted any time soon. Moreover, further tensions in other jurisdictions could lead to attacking oil giants in those regions; China, for example, could be a key focus in the future as diplomatic relations with western powers continue to sour.

Software companies

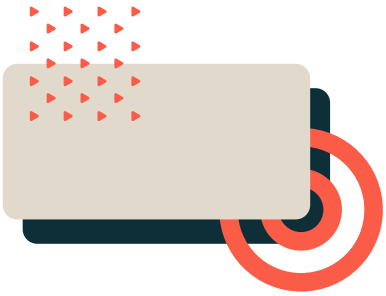
The rise of Internet-based businesses has provided a new set of challenges for companies with regards to their third-party management. For example, let's take a look at software-as-a-service ("SaaS") companies. As a relatively nascent industry, and one that continues to evolve rather rapidly, certain compliance best practices are still taking shape compared to more mature industries. For one, a software company typically operates heavily online and its onboarding processes for customers, suppliers, and other third parties can happen near instantaneously—and customers especially typically expect very expedited onboarding times.

Furthermore, these companies provide a product that can be "shipped" over the Internet and does not need to be physically delivered. As such, SaaS companies, for example, may never obtain an address from a customer, which many companies utilize to ensure the customer is not in a region subject to an embargo or otherwise blacklisted. By operating over the Internet, the entire transaction— from order to delivery—can occur near instantaneously, with limited intermediaries, and without regard for physical location or other barriers.

Further complicating things for software companies, the Internet offers ways for sanctioned actors to operate pseudonymously (sometimes outright anonymously) or to simply disguise themselves in a manner that is otherwise unproblematic. Bad actors have access to a slew of privacy tools now, such as virtual private networks ("VPNs") and onion routers that allow themselves to hide key identifying information such as their IP address, or to "spoof" their IP address to make it look like it comes from a non-sanctioned country. This presents a whole host of difficulties for SaaS companies that seek to comply fully with OFAC regulations. Many software companies already struggle in this regard, and privacy-enhancing technologies will only continue to improve.



Despite these challenges, software companies have access to new technical solutions to mitigate these unique risks. To some extent, Internet-based business may have some advantages, such as the ability to incorporate additional technological solutions in its compliance procedures, as well as increase automation. First and foremost, software companies should implement an automated platform that can perform screenings and analysis in real-time, just as swiftly as your platform can service your customers. An advanced screening platform can be implemented seamlessly into the customer onboarding process to thoroughly screen and re-screen relevant customer information, while minimizing data quality issues, such as common misspellings of names or addresses. In addition, software companies should generally look to implement the following controls:



- Conduct sufficient trade sanction due diligence on distributors, suppliers, and other intermediaries to identify ties to sanctioned countries and individuals;
- Conduct regular audits to evaluate the strength of internal controls;
- Conduct pre-acquisition trade sanction compliance-based due diligence and post-acquisition review and integration when acquiring new businesses; and
- Employ geo-location IP screening technology that has the ability to block IP addresses linked to prohibited countries

Utilities sector

Foremost among the myriad of risk factors facing the utilities sector is interactions with the foreign jurisdictions in which they operate. Since state-ownership of utilities—whether in whole or in part—is the norm in most parts of the world, companies subject to the FCPA, UK Antibribery Act, and other international anti-corruption laws face an elevated risk of engaging in quid pro quo transactions that contravene these laws.

Accordingly, companies operating in the utilities sector—whether providing energy generation and transmission services of their own or working in concert with those who do—must be careful about screening all third parties with whom they choose to conduct business to identify any potential governmental ties. This is particularly true for service providers with critical dealings in the Russian Federation, Belarus, and Ukraine, where the latest sanctions activity may frustrate, complicate, or altogether preclude businesses from providing any services with the capability of enhancing Russia's ability to wage continuous war.

Consequently, companies operating in the utilities space must adopt robust due diligence and third-party screening solutions that identify with clarity the beneficial ownership structure of any proposed counterparty. Crucially, such screening solutions should also be capable of identifying governmental affiliations on the part of key owners or counterparty officials that would also raise anti-bribery and corruption concerns. While businesses may not be liable for dealing with prohibited parties representing unsanctioned parties (e.g., the individually sanctioned CEO of an otherwise unsanctioned energy company) depending on the circumstances, such dealings can be a broader indicator that the proposed relationship poses a heightened risk from a sanctions perspective. This should factor into a company's decision about whether to undertake the business dealing in question, and if so, what risk mitigation efforts are the most appropriate to adopt under the circumstances.

> **"Companies operating in the utilities space must adopt robust due diligence and third-party screening solutions that identify with clarity the beneficial ownership structure of any proposed counterparty"**

An additional risk factor facing the utilities sector is increased restrictions on the ability of many companies to export components and other equipment critical for the operation and maintenance of utilities infrastructure. As export controls in the United States, European Union, and the United Kingdom increase, the ability of companies to export components subject to these restrictions to parties in Russia, Belarus, and certain rebel-controlled parts of Ukraine is limited. As the United States government announced earlier this year, all exports to Russia and Belarus falling within the scope of the Export Administration Regulations ("EAR")—with few exceptions—now require a license and are subject, in many instances, to a policy of denial.

This risk factor also underscores the need for organizations to invest now in third party screening solutions that have access to the latest regulatory updates. While many companies may have relied on manual screening solutions in the past, the sheer pace of regulatory developments in a post-Ukraine invasion environment makes it imperative that organizations wishing to avoid becoming a test case for prosecutors invest now in more robust, accurate, and efficient automated screening solutions.

Pharmaceutical sector/medical device industry

Pharmaceutical and medical device companies, too, face their own unique set of challenges in engaging third parties. This risk arises primarily from an anti-bribery and corruption standpoint. Because many foreign hospitals, research institutions, and clinics are wholly or partly owned by governmental entities, the risk of running afoul of the FCPA's anti-bribery provisions, for instance, is considerable.

> **"Complicating matters further is the simple fact that a majority of FCPA enforcement actions to date involve intermediaries often used by pharmaceutical and medical device companies to enter new markets or expand theirpresence in existing markets."**

Here, a robust internal reporting system must be maintained to permit both employees (and potentially external parties as well) to report on any such misconduct.

While any number of companies purport to offer basic hotline systems capable of meeting regulator expectations, the most compliant organizations will seek to implement hotline systems with integrated case management capabilities. This allows organizations operating in the pharmaceutical sector and medical device industry to maximize the compliance function's efficiency.

When intake and investigative processes are bifurcated, crucial elements of the initial complaint, supporting documentation and other evidence of potential malfeasance could be misplaced or lost entirely. Conversely, integration of these capabilities permits pharmaceutical and medical device companies to seamlessly prioritize, track, investigate, and disposition compliance complaints by utilizing a single platform.

The increasing focus of competent authorities on recovering monies from entities that illegally profited from COVID-19 and its immediate aftermath is another major risk factor facing the pharmaceutical sector and medical device industry. Massive expenditures on COVID testing and personal protective equipment often came without restrictions as governments worldwide struggled with containing the pandemic.

As the COVID crisis has waned in its severity, these governments—including the United States government—have prioritized the return of monies deemed to have been illegally siphoned by unscrupulous organizations masquerading as having provided legitimate COVID-related services to the public. To that end, in March 2022, the U.S. Department of Justice announced the appointment of a new Director for COVID-19 Fraud Enforcement.

While the immediate focus of the COVID-19 Fraud Enforcement apparatus has initially been on large-scale criminal enterprises and malign foreign actors, the prioritization of such a recovery effort by the nation's chief law enforcement agency should serve as a prescient reminder to all healthcare organizations that a robust internal reporting system is central to fulfilling an organization's commitment to compliance with all applicable laws and regulations. Pharmaceutical and medical device companies that lack such a system may find themselves in the unenviable position of having what would otherwise have been an internal report to the company's compliance team becoming an external one to regulators.

Adding to the urgency of adopting a robust internal reporting system and fostering a so-called 'speak up culture' is the stark reality that federal law incentivizes whistleblowing in relation to the alleged misuse of public appropriations. The federal False Claims Act, for instance, empowers private citizens to initiate qui tam actions against those who have defrauded the government and entitles them to receive a portion of any successful recovery in litigation. According to the Department of Justice's own statistics, qui tam actions have comprised a significant percentage of the Civil Division's fraud recovery efforts since 1987. In 2021 alone, the Department of Justice recovered nearly $5.6 billion in settlements and judgments in qui tam proceedings.

As of the fall of 2022, federal prosecutors have also been dogged in pursuing criminal convictions of those responsible for orchestrating COVID-19 testing fraud. Among the more notable convictions secured by the federal government was that of Mark Schena, the president of a Sunnyvale, California-based allergy and COVID testing company. According to documents filed in the U.S. District Court for the Northern District of California, Schena engaged in a pattern of deceitful conduct designed to mislead investors into believing that he had developed a COVID-19 testing solution that utilized dry blood samples. In actuality, no such testing solution existed, and Schena and his company illegally benefited from the submission of nearly $69 million in false and fraudulent claims for COVID-19 testing.

On September 1, 2022, a federal jury convicted Schena on all counts raised by the superseding indictment filed in the case, including health care fraud and conspiracy to pay kickbacks in connection with false and fraudulent statements made in connection with the regulatory status and accuracy of his COVID-19 test. The conviction of Schena is part and parcel of the Biden Administration's focus of holding individuals at the center of corporate misconduct responsible for their criminal acts. Schena's conviction underscores the importance of ensuring that statements made by health care organizations concerning COVID-19 products are accurate and supported by empirical evidence.

Manufacturing Sector

Manufacturers aare currently experiencing more regulatory and legislative scrutiny than at any other time in recent history. Driven in large part by the effort to infuse meaningful Environmental, Social and Governance ("ESG") standards into corporate culture, manufacturers are often the target of enhanced due diligence requirements that require the organization to mitigate its overall impact on the environment and socially undesirable outcomes like forced labor and human trafficking.

This year, the emphasis on the need for such due diligence became even more urgent as the Congress passed (and the Biden Administration began to implement) the provisions of the Uyghur Forced Labor Prevention Act ("UFLPA"). The UFLPA establishes a statutory presumption—albeit rebuttable—that the importation of any goods, wares, articles and merchandise mined, produced or manufactured wholly or in part in the Xinjiang autonomous region of the People's Republic of China ("PRC") is prohibited by Section 307 of the Tariff Act of 1930 based on the assumption that such goods and wares were produced using forced labor. The UFLPA creates a bright line rule that such products are categorically excluded from legal entry into U.S. territory.

Violations of the UFLPA render illegal shipments subject to seizure and subsequent forfeiture by U.S. Customs and Border Protection ("CBP").

To ensure compliance with the UFLPA—and other existing and emerging regulatory schemes that attempt to shed light on the entire value chain—manufacturers are required to conduct appropriate due diligence.

While ad hoc screening of counterparties may have been sufficient in the past, the UFLPA, California's Transparency in Supply Chains Act, and a host of other laws and regulations require all organizations (including manufacturers) to conduct appropriate risk-based due diligence concerning the origin and production of raw materials used in popular products.

> **"Organizations must conduct appropriate risk-based due diligence concerning the origin and production of raw materials used in popular products."**

Here again, compliance teams affiliated with global companies that are either partly or wholly reliant on manual screening processes are likely to find that their due diligence burden is impossible to bear in this new regulatory climate. This makes adopting a third-party screening solution with the capability of interfacing with a company's purchasing system all the more critical for manufacturers striving for efficiency in its compliance obligations. Partnering with a well-established compliance solutions company also means that such organizations can leverage additional expertise when needed. For instance, if a particular supplier is new to the manufacturing company and operates in a country posing an elevated risk, its compliance solutions provider can be retained to conduct enhanced due diligence at the organization's behest. Such enhanced due diligence reports can shed critical insight into the organization's beneficial ownership structure, financial condition, regulatory enforcement history, and legal status. These reports, in turn, can be relied on by the company's compliance function to assess and prioritize the risk associated with engaging that particular materials provider holistically.