Published on *The National Law Review* https://natlawreview.com

Sanctions and Cyber and Crypto, Oh My: The Convergence of Emerging Regulatory and Enforcement Risks Requires Nimble Responses Across Sectors

Article By:

Seth D. DuCharme

Claire E. Cahoon

Meagan C. Maloney

At a sanctions conference held in Washington D.C. on May 5, government officials, practitioners and corporations highlighted the government's broadening focus on anti-corruption enforcement, across more traditionally siloed areas. While Russian sanctions are a hot topic in and of themselves, government representatives across agencies noted that even aside from measures resulting from Russia's invasion of Ukraine, the United States has been steadily heightening its expectations regarding companies' creation, implementation, and supervision of anti-money laundering ("AML"), Foreign Corrupt Practices Act ("FCPA"), ESG and sanctions compliance programs.

The conference was an important reminder of the six critical areas that companies need to address in cross-coordinating their compliance efforts:

- Sanctions (U.S., U.K., E.U. and comparable regimes)
- Anti-Money Laundering (to include cryptocurrencies)
- Anti-Bribery (Foreign Corrupt Practices Act diligence)
- Commerce Controls (CCL and IEEPA concerns)
- State Department Licensing Requirements (Arms Export Control Act and ITAR)
- ESG (with strong focus on internal controls)

In this ongoing whole-of-government approach to anti-corruption, national security, and foreign policy, the United States continues to accelerate the use of sanctions and other initiatives, such as the creation of multiple task forces, to turn up the temperature on Russia and other foreign adversaries

as well as the private sector. But today's compliance risks today don't look quite the same as they did in years past, now presenting an assortment of arrows in the government's growing quiver.

Over the last few months, the Office of Foreign Asset Control ("OFAC"), has become increasingly active with initiatives that arguably have supplanted AML and FCPA diligence as the lead concerns for entities engaging in cross-border transactions. Notably, Andrea Gacki, Director of OFAC Enforcement, has highlighted a more interdisciplinary, interagency approach to sanctions enforcement in the coming year.[1] In her keynote address at the conference, Gacki confirmed that cyber and virtual currency are a top priority for OFAC, and that the agency will focus on technology, virtual currency, and non-financial industries. The White House similarly confirmed that the administration is focused on staying ahead of new and emerging trends in sanctions avoidance and is implementing an interagency strategy to enforcement.

Not surprisingly, Gacki also stressed that "it's never too soon to build a sanctions compliance program," reminding corporations that the government has high expectations for internal controls.[2] Most companies know that proactive and thorough compliance programs are critical in the AML and FCPA space, but as novel compliance issues, such as the continued increase in ransomware attacks and the accessibility of cryptocurrencies, challenge existing programs, it becomes increasingly difficult to have confidence that all areas of transactional risk are being effectively addressed.

It's no wonder that many companies are expressing increased concern about meeting government expectations and feeling pressure to strengthen compliance efforts on a wide range of related topics. Addressing these concerns largely boils down to effectively figuring out with whom you're doing business, where your products and services are going, and the collateral consequences that could flow from those transactions. Often, the business interest analysis must include a consideration of the rocky sea of evolving regulation, and a realistic assessment of short- and long-term risk arising from government action.

In light of these developments, companies should consider approaching compliance with a broader mandate, evaluating overlapping risks and ensuring that counsel and other outside advisors are looking beyond any one narrow issue. Subject matter expertise is critical, but silos of expertise may result in failing to detect red flags. The ideal strategy would be one that mirrors the government's interdisciplinary approach to anti-corruption and sanctions enforcement.

Over the last year, Bracewell has provided guidance about the steadily increasing efforts by the Biden administration to bring more scrutiny on corporate conduct, including OFAC's heightened expectations for companies' anti-money laundering and "know your customer" programs; export control risks related to OFAC sanctions risks; OFAC's increased scrutiny of ransomware payments; the Biden administration's continued focus on anti-corruption, particularly illicit domestic and international financing; the DOJ's aggressive new approach to monitoring corporate compliance; and more. From sanctions to anti-corruption and beyond, our lawyers are available and prepared to holistically advise clients on these and countless other compliance and enforcement concerns.

FOOTNOTES

1. The pointy ends of sanctions enforcement are the criminal investigations by the Department of Commerce, FBI, and the Department of Homeland Security into violations of International Emergency Economic Powers Act, which are prosecuted by multiple DOJ components, task forces and U.S. Attorneys' Offices.

[2.] Recent pronouncements from the Departments of Justice, State, Commerce, and Treasury emphasize the higher expectations and burdens on know-your-customer, anti-money laundering and internal controls practices. UK and EU regulators are taking a similar approach, adding to the complexity of gaining confidence in the ultimate propriety of cross-border transactions.

National Law Review, Volume XII, Number 136