

Enforcement Trends 2025: Magic 8 Ball Says “Try Again Later”

Update

December 09, 2024 | 6 minute read

As the world prepares for the change of administration in January, current government officials and industry experts convened at the New York Forum on Economic Sanctions to reflect on enforcement trends in 2024, and to speculate about the year ahead. While each regulator was careful to say they did not have a crystal ball view into what the future holds, there was universal agreement that sanctions and export controls will remain powerful enforcement tools, and the machinery that has increased inter-agency coordination is likely to remain in place.

Below we highlight key observations from the Justice Department’s National Security Division (NSD), the Commerce Department’s Bureau of Industry and Security (BIS), and the Treasury Department’s Office of Foreign Asset Control (OFAC) and discuss how companies can best position themselves in this time of transition. Highlights include:

- Continued close coordination among agencies
- Increasing focus on technology
- Evolving application of sanctions approaches
- Role of cryptocurrency
- OFAC’s efforts to modernize

Enhanced Coordination

Dan Clutch, Deputy Director of the Office of Export Enforcement at BIS, put succinctly what each regulator expressed in some fashion: in his 24 years of government service, he has never seen the type of coordination that currently exists among the various agencies and task forces, and he doesn’t see it going

Related People

Seth D. DuCharme

Partner

NEW YORK

+1.212.508.6165

seth.ducharme@bracewell.com

Margaret B. Beasley

Senior Counsel

NEW YORK

+1.212.508.6180

margaret.beasley@bracewell.com

Related Practices

[Government Enforcement &](#)

[Investigations](#)

[Litigation](#)

away as leadership transitions: “it’s for real, and it’s here to stay.” This close coordination began following Russia’s full-scale invasion of Ukraine in February 2022, with the creation of several joint task forces and increased information sharing. Now, almost three years later, it is clear that the agencies have developed highly effective working relationships and have become adept at leveraging their specific expertise to bring enforcement actions of all kinds.

For example, BIS Assistant Secretary Matthew Axelrod confirmed that in the past year his team reviewed more than 1,200 Suspicious Activity Reports from Treasury’s Financial Crimes Enforcement Network, and actioned more than 150 of them. He also reported that there was a 50 percent increase in charged cases as a result of the Disruptive Technology Strike Force, which is a joint effort among DOJ, Commerce, the FBI and HSI, and predicted more joint resolutions, such as that brought by OFAC and BIS against Microsoft for violations of both sanctions and export controls.

Another form of close coordination has been through sharing of information in voluntary self disclosures (VSDs). In the past few years, most regulators have implemented VSD programs under which companies may receive significant benefit for coming forward upon discovery of violations. ***The regulators confirmed that they regularly share VSDs with their colleagues at other agencies, such that companies should assume that information shared in a VSD to one agency means all have the information.*** Significantly, however, companies will only receive credit from the regulators to which they themselves make a VSD, meaning that companies should make VSDs to all potentially relevant agencies.

Relatedly, BIS highlighted two new features of its VSD program: (1) BIS will now consider it an aggravating factor if a company was aware of misconduct but did not self-report; and (2) BIS will provide “credit in the bank” for companies that provide credible, actionable tips on misconduct by industry competitors. These changes have increased both significant VSDs as well as actionable industry tips.

Ian Richardson, NSD’s Chief Counsel for Corporate Enforcement, spotlighted NSD’s first-ever declination under its VSD policy for sanctions and export controls violations. Richardson explained that although NSD’s policy provides for a presumption of a non-prosecution agreement, in this case the company’s self-disclosure was “textbook perfect” so DOJ felt it was appropriate to reward it with a full declination. He noted that the company came in exceptionally early, and proactively provided information that led to guilty pleas by two employees. This result demonstrates that the benefits of self-disclosure and full cooperation are real, even for national security-related violations.

Focus on Technology

One area of significant partnership among agencies is an increased focus on key and emerging technologies. Multiple panelists asserted that we are at pivotal national security moment with foreign adversaries attempting to access these technologies that will shape our future as a country, and the balance of power in the world.

DOJ highlighted the success of the Disruptive Technology Strike Force in addressing transshipment networks that convey micro-electronics overseas in violation of export controls, such as a [November 2024 resolution](#) with the founder and former chief executive officer of a California-based international logistics and freight forwarding company that pleaded guilty to conspiring to violate export laws by shipping goods to Chinese companies on BIS' Entity list, and a September 2024 [indictment](#) against two defendants who allegedly utilized shell companies, fictitious personas, and falsified records to help Russia obtain American-made laser welding machines in support of Russia's nuclear program. DOJ asserted that more such actions were on the way. We'll see.

This time last year, [we discussed](#) the rising importance of export controls, explaining that the targeted, agile, and less political nature of the Export Administration Regulations (EAR) provide the government with a new layer of regulations well-suited to this technology-focused threat. The regulators observed that, more and more, inclusion on BIS's End User Restriction list is akin to inclusion on OFAC's SDN list. DOJ also discussed coordination with Commerce specifically in actions abroad, warning that although sometimes DOJ runs into problems with dual criminality — where a foreign jurisdiction does not recognize an action as criminal — DOJ has “creative lawyers and ways of getting the information we need” from other angles and partners.

A new twist to protecting technology is that much of it is no longer physical, but rather information that can be transmitted, by an accomplice or through a spearfishing attack, over the internet. In these cases without a transshipping middleman, regulators have found an enforcement angle in the payment. This shift, in part, prompted BIS to develop guidance for the financial industries sector, issued on October 9, 2024, recommending that financial institutions undertake specific compliance practices to minimize their risk of violating General Prohibition 10 of the EAR. BIS emphasized that while these suggestions were not required, regulators would consider the failure to incorporate these or similar measures if a violation did later occur, because knowledge in this context goes beyond actual knowledge, and can be inferred from circumstances surrounding a transaction; in other words, a “known or should have known” standard.

Shifts in Sanctions Approach

Michael Khoo, the Co-Director of DOJ's Task Force KleptoCapture, discussed the evolution of sanctions tools to reflect changes in the enforcement

environment. For example, he said that while the initial focus of many agencies was the primary “bad guys” such as oligarchs and arms dealers — and their movable assets, such as luxury yachts — agencies are pivoting to actions against the army of professional facilitators such as transshippers, lawyers, bankers and corporate services providers that allow the primary bad actors to hide assets and move goods.

Similarly, following the initial wave of enforcement actions, regulators continue to consider whether parallel actions are necessary to fully accomplish their goal. For example, in early December, the Southern District of New York, in cooperation with DOJ and the FBI, [filed a civil forfeiture complaint](#) against more than \$3.4 million in proceeds from the sale of a music studio in Burbank, California, alleging that the proceeds, which are beneficially owned by Russian oligarch Oleg Deripaska, are the proceeds of sanctions violations. The action was taken despite an indictment charging Deripaska with sanctions violations had already been unsealed on September 29, 2022, and Deripaska remains at large.

Crypto’s Facilitation Role

Khoo expressed surprise that his team did not encounter more crypto assets when pursuing oligarchs, finding that their wealth was largely comprised of luxury goods or fiat holdings. However, he said that crypto is becoming highly relevant on the procurement side of enforcement efforts. Foreign entities seeking to obtain US technology have begun to realize that paying for such goods with USD or through US banks is too risky, and have turned to USD-pegged stable coins to process these transactions, benefitting from the credibility of USD while avoiding the jurisdiction of US regulators. He said that his team is looking at this trend closely, and leveraging the expertise of the [National Cryptocurrency Enforcement Team](#) as necessary.

Michael Grady, Chief of the Banking Integrity Unit of the Money Laundering and Asset Recovery Section at DOJ, discussed recent actions against crypto currency exchanges such as [Binance](#) for failure to comply with Anti Money Laundering (AML) regulations, and predicted such prosecutions will be a priority in the coming year. He added that AML is so crucial because it is not just a national security tool, but it also a screening measure for any other potential violation, such as sanctions, terrorism financing and export controls.

OFAC Modernization

Joshua Jungman, Policy Chief Compliance Division OFAC, spoke about the office’s recent modernization efforts, all geared at presenting a more unified message and more helpful information to industry. He highlighted the Office’s new compliance portal through which industry can seek guidance, saying that

this new approach will allow his office to provide faster responses to simple questions, elevate the harder questions to the right stakeholders, and allow leadership to see the areas that need more guidance. OFAC is also in the process of refreshing its FAQs, and in the coming months will be putting out more information via a video series and its blog. Jungman indicated that OFAC has heard industry requests to decrease reporting requirements, but said that change won't be happening any time soon, as it views the information as crucial to fulfilling its mission.

Takeaways

New leadership in the incoming administration will undoubtedly make some changes, but companies should not expect a dramatic shift in the enforcement space as it relates to prioritizing the national security of the United States, particularly with respect to Iran, China and Central America. Companies should continue to enhance their due diligence and compliance programs to reflect shifts in the global risk environment including by examining shipping and payment networks and ensuring visibility into the ultimate end users of their products or services. Corporate enforcement tools that were developed and refined by the outgoing administration are likely to be retained and employed by the new team.