Blogs
March 03, 2023

On March 2, 2023, U.S. Department of Justice Deputy Attorney General (DAG) Lisa Monaco once again delivered groundbreaking remarks at the American Bar Association National Institute on White Collar Crime, this time heralding a new era of corporate enforcement aimed at addressing U.S. national security priorities.

Last spring, as U.S. sanctions against Russia rolled out, DAG Monaco described sanctions as "the new FCPA (Foreign Corrupt Practices Act")" in terms of DOJ priorities, sending shockwaves through the world of corporate compliance. Since then, DOJ has borne that promise out largely through an aggressive campaign, championed by Task Force KleptoCapture, as we have previously written about, resulting in a large number of criminal cases targeting individual defendants.

In this most recent announcement, DAG Monaco set a new tone: announcing that enforcement of national security-related violations—most notably sanctions evasion and export control violations—against ***corporations*** would be among the top priorities of the DOJ. Later in the day, Matthew Axelrod, Assistant Secretary for Export Enforcement within the Department of Commerce, Bureau of Industry and Security (BIS), drove home that point, emphasizing that companies should no longer view export control and sanctions violations as "technical violations," but would be well advised to view them as enterprise risks given the prioritization these issues are receiving within the various government enforcement agencies, including the DOJ. Further highlighting this new landscape, the Department of Treasury Office of Foreign Assets Control (OFAC) spoke at the ABA White Collar Conference for the first-time ever on March 2 and the DOJ, BIS and OFAC issued their first-of-its kind joint compliance guidance the same day, relating to third party-intermediary risks.

It was a day filled with sea-changing announcements for sanctions and export control enforcement, but the takeaway was simple: ***Sanctions and export controls really are the new FCPA in terms of corporate enforcement priorities and related compliance expectations.*** The Money Laundering and Asset Recovery Section (MLARS) has already begun conducting sanctions- and export-related investigations.

New and Improved DOJ National Security Division

In her remarks, DAG Monaco suggested that DOJ will be working to add capabilities to the National Security Division (NSD) similar to the Fraud Division, which has had significant success in prosecuting FCPA violations against corporations over the past few decades. NSD's Counterintelligence and Export Control Section (CES), formerly the Counterespionage Section, has always handled complex white-collar cases such as economic espionage and export control violations, and that longstanding expertise will likely be expanded and supported by substantial additional bandwidth. DAG Monaco shared details as to several significant changes to DOJ NSD that will herald a new era of corporate enforcement focusing on national security priorities, including:

- Shifting the focus from terrorism-related crimes (which typically involve individuals and non-state actors) to threats related to state-sponsored activities (such as by Russia, China and North Korea), which more heavily implicate cross-border corporate activity;
- Adding more than 25 new prosecutors to NSD;
- Adding a new Chief Counsel for Corporate Enforcement role at NSD; and
- Issuing joint guidance with BIS and OFAC relating to corporate compliance expectations.

New Guidance on Third Party Intermediaries and Compliance

Beyond the recent slew of Task Force KleptoCapture enforcement actions, the enforcement community further evidenced its conviction to this mission by issuing the unprecedented joint corporate compliance guidance relating to sanctions and export control compliance the same day as DAG Monaco's announcements.

This guidance, promulgated jointly by DOJ, OFAC and BIS (the "Agencies"), focused on steps companies can take to mitigate the risks of sanctions and export control violations involving third-party intermediaries, such as agents, intermediary customers, distributors, etc.), who may facilitate efforts by other parties to evade U.S. restrictions. The guidance sets out a series of red flags to help businesses identify when third-party intermediaries may be engaged in efforts to evade sanctions and export controls, including notably:

- Use of corporate vehicles to obscure (i) ownership, (ii) source of funds, or (iii) countries involved, particularly sanctioned jurisdictions;
- Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration;
- Internet Protocol (IP) addresses that do not correspond to a customer's reported location data;

- Payment coming from a third-party country or business not listed on the End-User Statement or other applicable end-user form;
- Transactions involving entities with little or no web presence; and
- Routing purchases through certain transshipment points commonly used to illegally redirect restricted items to Russia or Belarus (e.g., China (including Hong Kong and Macau); Armenia, Turkey, and Uzbekistan).

The guidance also advises caution with respect to entities that use complex sales and distribution models, as this may obscure visibility into the ultimate end-users of an organization's technology and services. While the list of red flags in the guidance is not exhaustive, it reflects factors U.S. enforcement agencies will focus on when evaluating corporate compliance relating to the involvement of intermediary entities.

New Compliance Program Expectations

In addition to the red flags, the guidance re-emphasized the corporate compliance program expectations set out in prior guidance from the Agencies—including the OFAC guidance titled "A Framework for OFAC Compliance Commitments," issued in May 2019. The guidance also provides new clarification as to the compliance program expectations on organizations. In particular, organizations' risk-based compliance programs must be "effective," as described in the guidance. The guidance does not expressly define the term "effective" or how an organization will be assessed for "effectiveness," but it provides that an "effective" risk-based compliance program should include management commitment (including compensation incentives), risk assessment, internal controls, testing, auditing and training. "Effective" compliance programs employ a risk-based approach to sanctions and export controls compliance by developing, implementing, and routinely updating a compliance program, depending on the organization's size and sophistication, products and services, customers and counterparties and geographic locations.

The guidance clarifies the Agencies' due diligence expectations within an organization's risk-based compliance program, and specifically provides that as a "best practice" due diligence should not only be conducted on an organization's customers, but also on intermediaries and counterparties that are involved in customer transactions. In this regard, the guidance notes that optimal compliance programs should include controls tailored to the risk the business faces, such as diversion by third party intermediaries.

The guidance also references "compensation incentives" as a component to an "effective" compliance program. DAG Monaco in her comments notes that she announced last September that the DOJ would examine corporate compensation programs to shift the burden of corporate malfeasance away from uninvolved shareholders onto those more directly responsible, and that companies should ensure that executives and employees are personally invested in promoting compliance. Nothing grabs attention or demands personal investment like having skin in the game, through direct and tangible financial incentives. DAG Monaco further noted that she asked DOJ's Criminal Division to talk to practitioners, to consult with regulators and to develop guidance on how to reward corporations with compliance-promoting compensation programs.

The guidance also highlighted the voluntary self-disclosure policies of each of the enforcement agencies implicated, emphasizing the benefits of adopting procedures designed to detect wrongdoing internally and voluntarily report to regulators.

What Does This Mean?

The upshot is that companies can expect that sanctions violations and export controls violations will be increasingly pursued with the same level of resources and vigor that we have come to expect from DOJ with regard to FCPA enforcement. DOJ has provided a helpful roadmap in explicitly modeling changes to NSD after the Fraud Section; companies should consider following suit by carefully updating and evaluating the

effectiveness of their existing risk-based compliance programs, as appropriate based upon the guidance, assessing their sanctions and export control risks and leverage their anti-corruption compliance infrastructure to prioritize these risk areas.

Authors

Jamie A. Schafer

Partner
JSchafer@perkinscoie.com 202.661.5863

Mason Ji

Associate
MJi@perkinscoie.com 206.359.6308

Barak Cohen

Partner
BCohen@perkinscoie.com 202.654.6337

Richard W. Oehler

Partner
ROehler@perkinscoie.com 206.359.8419

David Aaron

Senior Counsel
DAaron@perkinscoie.com

Ann M. Nagele

Partner
ANagele@perkinscoie.com 206.359.6121

James F. Vivenzio

Senior Counsel
JVivenzio@perkinscoie.com 202.654.6200

Explore more in

White Collar & Investigations Data Security Counseling and Breach Response
Blog series

White Collar Briefly

Drawing from breaking news, ever changing government priorities, and significant judicial decisions, this blog from Perkins Coie’s White Collar and Investigations group highlights key considerations and offers practical insights aimed to guide corporate stakeholders and counselors through an evolving regulatory environment.

View the blog