BRACEWELL

INSIGHTS

"Export Controls Are the New Sanctions" and Other Enforcement Trends for 2024

January 11, 2024

*By: **Seth D. DuCharme** and **Margaret B. Beasley***

2023 was a banner year in the sanctions space and regulators seem primed to continue that performance in 2024. In December 2023, numerous government officials and industry experts convened at the New York Forum on Economic Sanctions to discuss lessons learned and predictions for the year to come. The conference featured officials from numerous agencies, including the Department of Justice's National Security Division (NSD), the Treasury Department's Office of Foreign Asset Control (OFAC) and Financial Crimes Enforcement Network (FinCEN), and the Commerce Department's Bureau of Industry and Security (BIS). Key themes included:

- use of export controls as an increasingly key compliance tool;
- enhanced cooperation among agencies and allies abroad;
- increased engagement between regulators and the private sector, including voluntary self-disclosure and whistleblower programs; and
- enforcement focus on technology and other new areas.

Below we discuss what these trends mean and what companies need to know.

Export Controls as the "New Sanctions"

Regulators and industry experts alike emphasized the increasing utility of export controls, with more than one speaker quipping: "If sanctions were the new FCPA, export controls are the new sanctions." And for good reason — the Export Administration Regulations (EAR) are in some ways a more targeted, more agile, more compelling, and less political form of sanctions. For example, EAR Part 744, Control Policy: End-User and End-Use Based, consists of lists, similar to the SDN list, that can be expanded without much warning. Part 746, Embargoes and Other Special Controls, implements broad controls related to Iran, Cuba, and Syria, and item specific controls as to certain other destinations, akin to OFAC's country- and sector-based sanctions programs. And EAR General Prohibition 10 (15 CFR § 736.2(b)(1)), which prohibits proceeding with transactions with knowledge that a violation has occurred or is about to occur, is essentially an analog to OFAC's prohibition on Facilitation Payments. As demonstrated by the enforcement actions discussed below, regulators are indeed employing these tools. Thus, companies should ensure that their compliance functions address not only the "familiar" OFAC sanctions, but also these commerce-based corollaries.

Enhanced Cooperation Among Agencies

Every regulator emphasized the importance of new cross agency task forces to tackle emerging challenges. Ian Richardson, Chief Counsel for Corporate Enforcement at NSD, highlighted the success of ***Task Force KleptoCapture***, an interagency task force set up in early 2022 dedicated to enforcing the sanctions, export restrictions, and economic countermeasures that the United States imposed following Russia's invasion of Ukraine, as well as the newer ***Disruptive Technology Strike Force***, which was established in early 2023 to target illicit actors, strengthen supply chains, and protect critical technological assets from being acquired or used by nation-state adversaries. He indicated that the agencies have hired a significant roster of new prosecutors and agents to staff these teams.

John Sonderman, the Director of the Office of Export Enforcement at BIS highlighted the ***new Suspicious Activity Report (SAR) key term***, rolled out with FinCEN, for financial institutions when reporting possible attempts by entities or individuals to evade US export controls. Building on similar efforts by BIS and FinCEN to require SARs for transactions related Russia, the new key term — "**FIN-2023-GLOBALEXPORT**" — is to flag transactions that may involve *any* evasion of US export controls, not just those targeting Russia.

The officials also highlighted increased cooperation with their counterparts abroad. For example, one panel acknowledged the historic issue with lack of dual criminality of conduct and noted that, while that is changing as more countries are enacting sanctions, those sanctions programs trigger compliance requirements and challenges for multinational companies operating in the increasingly regulated spaces. Regulators said US agencies are trying to align with our allies to simplify and streamline expectations, such as adopting similar definitions for key terms. Further, OFAC now has an exchange program with its U.K. counterpart, OFSI, and both have increased cooperation with the EU counterpart, OLAF.

On the other side of the globe, as part of the Trilateral Agreement among the US, Japan, and South Korea, the countries will now ***conduct exchanges*** between the US Disruptive Technology Strike Force and Japanese and ROK counterparts "to deepen information-sharing and coordination across our enforcement agencies. We will also continue to strengthen trilateral cooperation on export controls to prevent our technologies from being diverted for military or dual-use capabilities that could potentially threaten international peace and security."

Indeed, Nathan Swinton, the Coordinator for the Disruptive Technology Strike Force cited the ***indictment of a Belgian national*** for a scheme to export military-grade technology to China and Russia as an example of these forces coalescing. Concurrent with the US indictment, the defendant was arrested by Belgian authorities and he and his companies were added to the Entity List by BIS and to the SDN List by OFAC.

Increased Engagement With the Private Sector

Regulators also doubled down on the importance of working with their regulatees and the private sector writ large. NSD emphasized that, at the end of the day, these are mission-driven organizations, so while they will certainly bring enforcement actions as needed, they would rather work with companies and only resort to actions against willful violators. It said that the Department's Voluntary Self Disclosure (VSD) Policy, under which companies that self-report violations fare much better, is meant to provide companies both an incentive to build strong compliance programs and, recognizing that no program will be perfect, to report violations that

do occur. OFAC added that VSDs are a mitigating factor in enforcement decisions, and that in cases where a civil monetary penalty is warranted, a qualifying VSD can result in a 50 percent reduction in the base amount of the proposed penalty. NSD also discussed the Department's new VSD program for M&A transactions, which ***Bracewell covered*** when it was announced late last year. And BIS highlighted the new dual-track VSD program at his agency, under which VSDs involving minor or technical infractions will be resolved on a "fast-track" with a warning letter or no-action letter within 60 days of receipt of a final submission, whereas VSDs that indicate potentially more serious violations will be assigned to both a field agent and an Office of Chief Counsel attorney for an in-depth investigation.

In a similar vein, BIS discussed its relatively new policy of non-monetary resolutions for less serious violations, indicating its efficacy and continued use. Under that approach, violators whose breaches do not pose "serious national security harm," but exceed a warning letter or no-action letter, will be offered non-monetary settlement agreement resolutions to rectify the violation in return for violators accepting responsibility, admitting to the conduct, and committing to enhanced compliance measures.

More robust whistleblower programs across the agencies were also a trend, described as "a key feature" going forward. OFAC noted that its compliance hotline led to 57,000 leads in 2022. FinCEN's Kaveh Miremadi touted Treasury's new whistleblower program, under which tipsters can receive up to 30 percent of the total recovery in all related enforcement actions stemming from their call. While BIS intends to release a Notice of Proposed Rulemaking in July 2024 to address remaining logistical issues, it said that even in its early days the hotline is already a "vibrant pipeline" and that roughly 40 percent of the tips were quality. This new incentive changes the calculus for companies considering a VSD: every day that a company waits and does not submit a VSD is a day that an employee could reach out via the whistleblower hotline.

Finally, all of the agencies said they anticipated increasing their proactive outreach to their respective constituencies and liaising with law enforcement agencies such as Homeland Security and the FBI to foster dialog, information sharing, and relationships.

Enforcement Trends: Technology and Beyond

The regulators highlighted a few 2023 settlements that previewed the types of enforcement actions we should anticipate in 2024, including a focus on FinTech and virtual currency, non-US companies and persons using the US financial system to transact with sanctioned entities, and expanding the range of industries in which they pursue actions.

Regarding enforcement targets, OFAC noted the Office's largest settlement to date against a *non-financial institution* — $508 million with ***British American Tobacco*** for apparent violations of two sanctions programs related to North Korea, as well as a notable settlement with a *natural person* who was alleged to have caused ***Murad*** to violate Iranian sanctions.

NSD said the recent ***Binance settlements*** demonstrate the agencies' increased focus on cryptocurrency and responsible executives, and their whole-of-government approach. That settlement, which requires Binance to pay more than $4.3 billion and plead guilty to AML and sanctions violations, was a joint effort among DOJ, OFAC, FinCEN, and the CFTC. Binance's former CEO, Changpeng Zhao, also pled guilty to AML violations and will pay a $50 million fine. Prosecutors allege that Binance failure to implement programs to prevent and report suspicious transactions with terrorists, ransomware attackers, money launderers, and other criminals, as

well as matching trades between US users and those in sanctioned jurisdictions. In a first for OFAC, the settlement also includes a five-year monitorship — a requirement OFAC said highlights the fact that Binance leadership was saying the right things but not doing them.

The focus on technology also implicates the rise of export controls. For example, BIS imposed a $300 million civil penalty against ***Seagate Technology LLC*** (California) and Seagate Singapore International Headquarters Pte. Ltd. (Singapore) to resolve alleged violations of the EAR's foreign direct product rule related to selling hard disk drives — both the disks themselves and the technology they contain — to Huawei, which is on the BIS List. Beyond being the largest standalone penalty in BIS history, the penalty also includes an audit requirement. Similarly, BIS imposed a $2.77 million penalty on 3D printing company ***3D Systems Corp***. related to its sending export-controlled blueprints for aerospace and military electronics to China. Notably, sending the technology to its subsidiary in China — even for US orders — was still considered an export of technology in violation of EAR. The penalty also includes an audit requirement.

Takeaways

While none of these trends represents a sea-change in regulatory practice or priorities, they do point to important shifts in agency resources and enforcement approaches. Companies will be well served by making New Years resolutions to evaluate their compliance programs across *all* regulatory regimes, enhance their contractual attestations regarding third parties and end-users, and get to know their local FBI/HSI agents *before* an event arises.

A version of this update was also published by Thomson Reuters' Westlaw Today on January 12, 2024.