

DOJ Strike Force Allegations Highlight Diversion and Theft from U.S. Companies

by Lawrence Ward, Dave Townsend, Nicole Engisch, and T. Augustine Lo

The U.S. Department of Justice (“DOJ”) on May 16 announced criminal charges and arrests that highlight risks for companies from U.S. and non-U.S. networks and individuals that seek to unlawfully divert U.S. goods, services, software, technology, and trade secrets. In all of the cases, the allegations made public by the DOJ involve U.S. companies and the misuse or diversion of sensitive goods, non-public information, or financial services. The allegations highlight ways in which U.S. companies may see their products and intellectual property (“IP”) unlawfully diverted to China, Iran, and Russia, including in ways that undermine the company’s IP or that risk reputational harm. The allegations stress the importance of a robust export controls compliance program and technology control plan. U.S. companies must be diligent about red flags and the possibility of threats from U.S.-based customers and even employees.

The DOJ announcement builds on a trend of increasing enforcement of U.S. economic sanctions and export controls and IP theft, including using criminal charges against individuals and corporations for violations of U.S. law. As we highlighted in an earlier update, the DOJ has launched a multi-agency *Disruptive Technology Strike Force* that is co-led by the DOJ and the U.S. Commerce Department. The Strike Force’s goal is to “counter efforts by hostile nation-states to illicitly acquire sensitive U.S. technology to advance their authoritarian regimes and facilitate human rights abuses.” The DOJ charges announced on Tuesday are the first cases brought by the Strike Force.

Particularly noteworthy are the types of U.S.-origin goods, services, software, technology, and IP at issue in these cases, and how they were allegedly unlawfully taken or diverted:

- **U.S. Defense and Dual-Use Items.** One set of allegations (*United States v. Bogonikolos*) involved procurement and diversion to Russia of electronics, testing equipment, and tactical battlefield equipment. According to the DOJ, some of the items involve quantum cryptography and nuclear weapons testing. The DOJ alleges the defendant, who claimed to be operating as a defense contractor for allied nations, violated U.S. export controls, economic sanctions, arms controls, and other U.S. law.

Related People

- Lawrence Ward
- Dave Townsend
- Nicole Engisch
- T. Augustine Lo

Related Capabilities

- Government Enforcement & Corporate Investigations
- Intellectual Property
- International Trade
- National Security Law

This case highlights the need for U.S. exporters to use heightened due diligence of foreign partners when sensitive goods are involved.

- **U.S. Aircraft Parts.** The DOJ also charged two Russian nationals (*United States v. Besedin and Patsulya*) with diverting aircraft parts to Russian airlines, including those that are subject to Temporary Denial Orders issued by the U.S. Commerce Department's Bureau of Industry and Security. The Russian individuals are alleged to have hidden the names of end-users in Russia to avoid corporate compliance programs from stopping shipments. The defendants are charged with violating laws regarding U.S. export controls and money laundering. This is the latest in a line of cases involving illegal Russian procurement networks, and the case highlights the need for U.S. exporters to remain vigilant as to "red flags."
- **U.S. Intellectual Property.** The DOJ has charged a California resident (*United States v. Li*) with taking trade secrets from his former employer relating to high precision measurement studies and point cloud technology, which are used in making 3D models, and with setting up a competing business in China. The DOJ alleges the defendant stole trade secrets in violation of U.S. law.
- **Autonomous Systems Source Code and Technology.** The DOJ alleges that an individual (*United States v. Wang*) took technology and source code from his employer, Apple Incorporated ("Apple"), after signing a contract to join a competing autonomous vehicle manufacturer in China. The complaint targets a former Apple employee involved with developing hardware and software for autonomous systems. The DOJ has charged the individual with theft of trade secrets.
- **U.S. Financial Services.** Another set of allegations (*United States v. Xiangjiang Qiao*) involve the diversion of isostatic graphite to Iran and using U.S.-based financial institutions to process transactions relating to transactions with Iran. Isostatic graphite is used in missile applications. The United States alleges that the defendant violated a number of laws, including U.S. sanctions and money laundering laws, and that the defendant committed bank fraud.

These cases highlight the need for U.S. companies to remain diligent and attentive to red flags as to potential diversion or theft of products and IP. The DOJ's press release notes collaboration among the DOJ, the Federal Bureau of Investigations ("FBI"), and intelligence resources to investigate allegations underlying the criminal charges.

Cooperation by U.S. companies undoubtedly also contributed to the cases. Under U.S. economic sanctions and export controls, companies can be liable for the unlawful diversion of their goods, services, software, and technology, even under circumstances where they lacked actual knowledge of diversion to restricted locations or persons. U.S. enforcement authorities have thus stressed the need for U.S. companies to maintain a robust compliance policy backed by testing and auditing to ensure company employees are aware of and investigate red flags. In addition, as highlighted in another recent update, current DOJ policies incentivize companies to voluntarily self-disclose criminal misconduct, cooperate with criminal investigations, and take steps toward timely and appropriate remediation. Once potential issues are discovered, companies need to carefully think through approaching or responding to the DOJ, the FBI and other U.S. law enforcement authorities.