September 14, 2023

Recent DOJ Announcement Signals Continued Surge of Resources to Combat Corporate National Security Crime

On September 11, 2023, the Department of Justice ("DOJ") announced the appointment of two veteran prosecutors, Ian Richardson and Christian Nauvel, to serve as the first Chief Counsel and Deputy Chief Counsel for Corporate Enforcement, respectively, in the National Security Division.[1] The new Chief and Deputy Chief Counsel have collectively served as lead prosecutors on significant prosecutions involving corporations alleged to have committed national security crimes, including in *United States v. Lafarge SA* (involving the first prosecution of a corporation for providing material support to foreign terrorist organizations) and *United States v. Huawei Technologies* (involving allegations of sanctions violations and theft of trade secrets), as well as in cases involving cybercrime, cyber-espionage, and cryptocurrency.[2] On September 11, the Chief Counsel explained that his responsibilities would include "introduce[ing] some consistency and predictability in how we approach corporate investigations in the national security space" and "help[ing] coordinate and drive National Security Division investigations of corporate wrongdoing."

The filling of these positions, created in March 2023, marks another milestone in the DOJ's recent efforts to surge resources to what the Deputy Attorney General has called "the increasing intersection of corporate crime and national security."[3] According to the DOJ, between October 2022 and May 2023, approximately two-thirds of the DOJ's "major corporate criminal resolutions have implicated United States national security."[4] The DOJ's increased focus on corporate national security matters has sometimes been characterized using the DAG's phrase that "sanctions are the new FCPA."[5] But even that focus on sanctions, although critical, understates the full scope of the DOJ's corporate national security efforts. As Principal Deputy Attorney General Marshall Miller explained, "companies in the private sector are on the front lines of the geopolitical and national security challenges that mark today's global environment. From money laundering and cyber- and crypto-enabled crime to

[1] DOJ, *Justice Department's National Security Division Announces Key Corporate Enforcement Appointments* (Sept. 11, 2023), available here ("DOJ Announcement").

[2] *Id.* Our prior memorandum previously described the prosecution of LaFarge and its implications for corporate criminal enforcement. *See* Paul, Weiss, *DOJ Brings First Terrorism Material Support Charge Against a Corporation, Underlining the Importance of Compliance When Operating in High Risk Countries and of Robust M&A Due Diligence* (Oct. 20, 2022), available here ("BAT Client Memorandum").

[3] DOJ, *Deputy Attorney General Lisa Monaco Delivers Remarks at American Bar Association National Institute on White Collar Crime* (Mar. 2, 2023), available here ("Monaco Remarks").

[4] DOJ, *Principal Associate Deputy Attorney General Marshall Miller Delivers Remarks at the Ethics and Compliance Initiative IMPACT Conference* (May 3, 2023), available here.

[5] Monaco Remarks.

sanctions and export control evasion and even funneled payments to terrorist groups, corporate crime increasingly — now almost routinely — intersects with national security concerns." Thus, as we have discussed in prior alerts, recent actions in this space, in addition to the *LaFarge* case, include the historic resolution with British American Tobacco for bank fraud and sanctions offenses related to North Korea,[6] and prosecutions by the Disruptive Technology Strike Force (which focuses on export control and theft of trade secrets) for theft of U.S. intellectual property to benefit foreign corporations.[7] Moreover, the Chief Counsel's broad reference to "driv[ing] National Security Division investigations of corporate wrongdoing" implicates the full reach of NSD's Counterintelligence and Export Control and Counterterrorism sections, which collectively investigate crimes related to espionage, sanctions and export control, cybercrimes, the Foreign Agents Registration Act, terrorism, as well as fraud and money laundering linked to national security matters.

The DOJ's increased focus on and resources for corporate national security crime has significant implications for a wide variety of companies:

- **All companies should consider their exposure to national security risks**. Even companies that do not traditionally think of themselves as having exposure to national security risks should re-examine their exposure and consider taking additional measures—including undertaking risk assessments, putting into place or enhancing policies and procedures, updated training, and ensuring contracts have sufficiently broad sanctions, export controls, and related provisions--to guard against national security-related enforcement risk.

- **Due diligence in M&A deals and across international supply chains is critical**. DOJ's increased, aggressive enforcement related to national crimes creates particular risks for companies engaging in M&A activity that touches on foreign jurisdictions, as well as for companies that rely on an international supply chain.

- **Companies with exposure to China, Russia, and other jurisdictions that are the focus of U.S. national security efforts should be particularly cautious.** As we have discussed, the DOJ (and the entire U.S. government national security apparatus) have paid particular attention to conduct involving China and Russia,[8] as well to countries with what the DAG has called "autocratic regimes." For example, the Biden Administration's August 2023 "Executive Order on Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern" again signals scrutiny of transactions related to China.[9]

* * *

[6] BAT Client Memorandum.

[7] Paul, Weiss, *First Cases from DOJ's Disruptive Technology Strike Force Cover Export Control Evasion and Trade Secret Theft* (Jun. 5, 2023), available here ("Disruptive Technology Strike Force Memorandum"). (Although the specific defendants prosecuted in these cases were individuals, the government alleged that the thefts were made to benefit various foreign corporations.)

[8] Paul, Weiss, *Deputy Attorney General Announces Creation of Disruptive Technology Strike Force* (Mar. 3, 2023), available here; Paul, Weiss, *DOJ Prosecutions Reflect Aggressive Stance Toward Russian Sanctions and Export Control Evasion* (Oct. 26, 2022), available here; Disruptive Strike Force Memorandum.

[9] Paul, Weiss, *President Biden Issues Executive Order Creating Unprecedented Outbound Investment Review Prohibitions Targeting China* (Aug. 10, 2023), available here.

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Jessica S. Carey
+1-212-373-3566
jcarey@paulweiss.com

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

David Fein
+44-20-7367-1608
dfein@paulweiss.com

Michael E. Gertzman
+1-212-373-3281
mgertzman@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Brad S. Karp
+1-212-373-3316
bkarp@paulweiss.com

Mark F. Mendelsohn
+1-202-223-7377
mmendelsohn@paulweiss.com

Peter Carey
+1-202-223-7485
pcarey@paulweiss.com

Richard S. Elliott
+1-202-223-7324
relliott@paulweiss.com

David K. Kessler
+1-212-373-3614
dkessler@paulweiss.com

Associate Joshua R. Thompson contributed to this Client Memorandum.