ALM | LAW.COM

New York Law Journal

WHITE-COLLAR CRIME

White-Collar Criminal Enforcement and National Security

November 8, 2023

By **Elkan Abramowitz**

And **Jonathan S. Sack**

White-collar criminal statutes range widely and reach practically every corner of public and commercial life. But, on the federal level, enforcement has often come (and gone) in waves of investigations and cases of similar type.

This is particularly true at Main Justice. Take, for example, the years of effort directed against financial statement fraud in the early to mid-2000s, misconduct related to the financial crisis of 2007–09 and Foreign Corrupt Practices Act (FCPA) violations in a variety of industries and countries. These trends in enforcement did not encompass the full extent of white-collar criminal prosecutions, to be sure, but they were dominant themes which affected the enforcement of white-collar crime generally.

We have entered a new phase of white-collar criminal enforcement at the federal level—at least based on what senior DOJ officials have told us over the past 12 to 18 months. In June 2022, following Russia's February 2022 invasion of Ukraine, Deputy Attorney General Lisa O. Monaco spoke of criminal enforcement of economic sanctions as a "sea change" in white-collar enforcement. She referred to sanctions as "the new FCPA."

Just recently, on Oct. 4, 2023, Monaco said that the Department of Justice's (DOJ) "message should be clear: the tectonic plates of corporate crime have shifted. National security compliance risks are widespread."

With new priorities has come a substantial increase in enforcement resources and enforcement actions. Much of the new funding has been directed to the National Security Division of DOJ and to the Money Laundering and Asset Recovery Section of the Criminal Division—not to the Fraud Section of the Criminal Division. These new priorities can also be seen in the Biden administration's record-breaking 2,500 new sanctions designations, mostly targeting Russian individuals and entities, which will doubtless lead to investigations and prosecutions.

This follows the Trump Administration's substantial number of new sanctions designations in 2018, which

ELKAN ABRAMOWITZ *and* JONATHAN S. SACK *are members of Morvillo Abramowitz Grand Iason & Anello. Abramowitz is a former chief of the criminal division in the U.S. Attorney's Office for the Southern District of New York. Sack is a former chief of the criminal division in the U.S. Attorney's Office for the Eastern District of New York.* EMILY SMIT, *an associate at the firm, assisted in the preparation of this column.*

targeted individuals and entities tied to Iran, North Korea, Venezuela and, to a lesser extent, Russia.

Alongside these national security enforcement initiatives, DOJ has emphasized, predictably, corporate compliance and self-reporting. The Criminal Division's corporate leniency policy encourages voluntary self-disclosure, cooperation and remediation by companies.

On top of that, DOJ announced a new department-wide leniency policy applicable to corporate merger and acquisition transactions. The Mergers and Acquisitions (M&A) Safe Harbor Policy encourages companies to disclose and remediate misconduct uncovered in connection with an acquisition.

In this article, after discussing DOJ's national security enforcement initiatives, we turn to several cases that have been identified as representative of this new focus. We next discuss DOJ's M&A Safe Harbor Policy and how it complements and reinforces DOJ's current voluntary disclosure policy. We close with thoughts about possible implications of harnessing white-collar criminal enforcement to help achieve broader government aims, in this case, national security policy.

DOJ announced that it intends to concentrate on money laundering, cyber-and crypto-enabled crime, sanctions and export control evasion, money laundering and terror finance.

The 'Sea Change'

In June 2022, Monaco compared DOJ's commitment to sanctions enforcement to the Criminal Division's recent expansive and aggressive enforcement of the FCPA. By March 2023, in an address to the ABA National Institute on White Collar Crime, Monaco described more broadly DOJ's "surge of resources" dedicated to the "increasing intersection" of corporate crime and national security challenges.

In the following months, senior DOJ officials reiterated the department's focus on the "significant and growing" threat that corporate crime presents to national security.

In response to that threat, DOJ announced that it intends to concentrate on money laundering, cyber- and crypto-enabled crime, sanctions and export control evasion, money laundering and terror finance. In a May 2023 address, Principal Associate Deputy Attorney General Marshall Miller explained that enforcement in these areas had already been significant and, in particular, that more than two-thirds of the DOJ's major corporate criminal resolutions from October 2022 to May 2023 implicated national security-related crimes.

In the second half of 2023, the increase in resources directed to national security enforcement came into focus. On June 20, 2023, DOJ announced the creation of the new National Security Cyber Section (NatSec Cyber) within the National Security Division. The new section will address cyber-related threats to national security, especially from China, Russia, Iran and North Korea, including the theft of sensitive technologies, trade secrets, intellectual property and personally identifying information, and threats pertaining to critical infrastructure and malign influence (*e.g.*, foreign interference with elections).

On Sept. 11, 2023, Miller announced two new supervisory positions in the National Security Division—Chief Counsel and Deputy Chief Counsel for Corporate Enforcement, established to oversee the investigation and prosecution of national security-related corporate crime.

Ten days later, Miller said that DOJ is in the process of hiring 25 new National Security Division prosecutors, and that DOJ's Bank Integrity Unit had hired six new prosecutors—a 40% expansion of the unit. The Bank Integrity Unit, part of the Money Laundering and Asset Recovery Section of the Criminal Division, focuses on the Money Laundering Control Act, the Bank Secrecy Act and economic and trade sanctions programs.

The national security initiative builds on other related DOJ efforts. For example, in March 2022, the DOJ announced formation of Task Force KleptoCapture following Russia's invasion of Ukraine. Foreign kleptocracy has been of importance to the Criminal Division for many years, largely coinciding with the Fraud Section's enforcement of the FCPA. The new task force is dedicated to enforcing sanctions, export controls and other economic countermeasures, such as seizures of assets and freezing of bank accounts.

In February 2023, the Disruptive Technology Strike Force was created to investigate and prosecute theft and unlawful use of commercial technological assets by nation-state adversaries, notably, China.

In light of the "sea change" in DOJ policy, particular care will be expected when an acquirer discovers potential misconduct that affects national security.

Representative Cases

DOJ officials have pointed to five cases as representative of the "sea change" in white-collar enforcement priorities. One that is mentioned frequently is the department's first-ever corporate guilty plea for material support of terrorists. LaFarge S.A., a French construction company, admitted in October 2022 to paying the Islamic State and an al Qaeda affiliate to keep a cement business in Syria in operation, which resulted in over $750 million in financial penalties. *See United States v. LaFarge*, No. 22-cr-444 (E.D.N.Y. 2022).

Two cases involve North Korea-related activity. In April 2023, British American Tobacco PLC (BAT) entered into a deferred prosecution agreement to resolve charges of bank fraud and sanctions violations for selling tobacco in North Korea, which generated revenue that advanced North Korean nuclear programs. *See United States v. British American Tobacco*, No. 23-cr-118 (D.D.C. 2023).

In May 2023, charges were unsealed against a North Korean official and China-based crypto launderers for a scheme in which workers used fake or stolen identities to secure work and launder transfers of their compensation to the North Korean regime. *See United States v. Sop, et al.*, No. 23-cr-129 (D.D.C. 2023).

In September 2023, the DOJ announced its first-ever criminal resolution for sanctions violations arising from illicit sales and transportation of Iranian Oil. Suez Rajan Limited, a shipping company, and its parent company, Empire Navigation, entered into a deferred prosecution agreement for violations of the International Emergency Economic Powers Act and Iranian Transactions and Sanctions Regulations issued under the Act. *See United States v. Suez Ranjan, et al.*, No. 23-cr-88 (D.D.C. 2023).

Over the past two months, the DOJ has charged Russian nationals with fraudulently obtaining from U.S. distributors large quantities of military grade microelectronics, with military applications to Russia, and concealing from the U.S. government and distributors that the microelectronics were destined for Russia. The defendants have been charged with export control violations, money laundering, conspiracy to defraud the United States and wire fraud, among other charges. *See, e.g., United States v. Marchenko*, 23-mj-6181 (S.D.N.Y. 2023). This prosecution is led by Task Force KleptoCapture and the Disruptive Technology Strike Force.

M&A Safe Harbor Policy

On Oct. 4, 2023, Monaco announced a "Safe Harbor Policy" for voluntary self-disclosures in connection with merger and acquisition transactions. The M&A Safe Harbor Policy has broad application, but one of its goals is to encourage self-reporting of corporate national security-related offenses.

Under the M&A Safe Harbor Policy, acquirers that promptly and voluntarily disclose criminal conduct within a "safe harbor" period, cooperate with DOJ investigation and conduct timely and full remediation

(including disgorgement), will be given a presumption of declination.

For the policy to be effective, DOJ recognizes that it must be transparent and predictable. To create transparency, the policy provides that aggravating factors at the target company will not adversely affect the acquiring company's request for leniency. Aggravating factors might be relevant, but only as to charging decisions regarding the target company.

To create predictability, the policy establishes timelines for disclosure. Acquiring companies must disclose misconduct at the acquired entity within six months from the date of closing on the transaction, regardless of whether the misconduct was discovered before or after acquisition. In the case of misconduct that affects national security or might cause imminent harm, disclosure must be made more quickly.

Companies have one year from the date of closing to remediate fully. These deadlines for disclosure and remediation may be extended based on a "reasonableness analysis."

The new Safe Harbor Policy is not without precedent. About 15 years ago, the FCPA Unit of the Fraud Section published an opinion explaining the basis for leniency in an acquisition made by Halliburton Company. However, the opinion applied only to the Halliburton transaction. The Safe Harbor Policy, by comparison, will apply department-wide to all types of criminal conduct. As Monaco observed, the DOJ does not want to "discourage companies with effective compliance programs from lawfully acquiring companies with ineffective compliance programs and a history of misconduct."

The "carrots" in the M&A Safe Harbor Policy come with an implied "stick." Acquiring companies that fail to disclose and remediate a target company's misconduct will likely face heightened risk of successor liability for an acquired company's misconduct.

In light of the "sea change" in DOJ policy, particular care will be expected when an acquirer discovers potential misconduct that affects national security. A company's pre-acquisition due diligence is thus of the utmost importance; it may enable an acquirer to get the benefit of the M&A Safe Harbor Policy and avoid the danger not simply of overpaying for a target company but of taking on criminal liability.

Conclusion

In earlier waves of white-collar criminal enforcement, a basic cause-and-effect relationship could be found. Once potential large-scale financial crimes occurred, law enforcement resources were deployed, and investigations and cases followed, as we saw with the dot-com bubble and the financial crisis, for example.

In the DOJ's emphasis on national security, we detect something a bit different and less straightforward. To be sure, threats to our national security are real and substantial, and the "sea change" in enforcement responds to real-world developments in white-collar criminal activity as well as news headlines.

But more so than in the past, the DOJ may be harnessing white-collar criminal enforcement to help implement another policy—here, national security policy—not just to respond to the detection of widespread white-collar criminal activity. White-collar criminal enforcement, a cumbersome tool at best, is being deployed as part of national policy more broadly.

Perhaps this development makes sense, especially given the public attention devoted to our relationships with Russia, China and other adversaries. But perhaps this development hints at a subordination of criminal law to other policies, and to politics more broadly. Maybe that has always been true, but maybe not to this extent. Our views are tentative, and we are keenly interested to see how the latest iteration of DOJ white-collar crime policy turns out.