BRACEWELL

INSIGHTS

Biden Administration Prioritizes Increased and Broadened Anti-Corruption Enforcement

June 9, 2021

*By: **Seth D. DuCharme**, **Matthew G. Nielsen**, **Jeffery B. Vaden**, and **Rebecca J. Foxwell***

On June 3, 2021, the White House issued a ***memorandum*** announcing anti-corruption as a core national security interest. The memorandum explains that, "[c]orruption threatens United States national security, economic equity, global anti-poverty and development efforts, and democracy itself." It directs an unprecedented interagency focus on combating corruption, and signals increased funding for these efforts.

Currently, investigations targeting business-related corruption are largely conducted by the Justice Department under the Foreign Corrupt Practices Act ("FCPA") (focusing on bribery of foreign officials), with the SEC looking for potential follow-on books-and-records violations in the case of publicly-traded companies. The June 3rd memorandum indicates that the status quo is almost certain to change. The national security advisor will lead a group of agencies to bring a new war against corruption, with recommendations due to President Biden by the end of the year. While it is not clear exactly what new law, rules, or initiatives will come, it is clear that how the federal government defines corruption and seeks to root it out will likely significantly change.

For instance, the June 3rd memorandum calls for addressing all forms of illicit finance in the United States and international financial systems, including by stepping up money laundering enforcement and implementing robust federal law requiring U.S. companies to report their beneficial owner or owners to the Treasury Department. The Biden Administration has also separately signaled an increased focus on cybersecurity, a hardline approach to China, and a continued focus on Sanctions, Export Controls, and the Foreign Agents Registration Act ("FARA").

While the Biden Administration's enforcement policies will continue to take shape over the coming months, companies should take action now to identify and address their risks that could expose them to an investigation or enforcement action. Although companies need to evaluate controls and processes to comply with sector-specific laws and regulations, here are some areas in which we expect to see an increased focus that affect most companies.

Foreign Corrupt Practices Act

The FCPA's anti-bribery provision prohibits offering, making, or authorizing a payment of anything of value knowing that it will be offered or given to a foreign official to obtain or retain

business. The FCPA's accounting provision requires companies with securities listed on stock exchanges in the United States to keep books and records that accurately reflect the transactions of the corporation and to maintain an adequate system of internal accounting controls. Subject to certain limitations,[1] the FCPA has extraterritorial application, meaning that both companies and individuals may be held liable under the FCPA for bribery that occurs anywhere in the world.[2]

Companies may be vulnerable to FCPA violations based on the countries in which they operate, the types of benefits they offer in the ordinary course of business, such as meals and entertainment, gratuities and gifts, and travel expenses, and the third-parties that they work with. It is important to remember that a company may be held liable not only for the corrupt actions of its employees, but also for the corrupt actions of a third party if the third party was acting on the company's behalf. Ninety percent of reported FCPA cases involve third parties. Potential penalties include significant corporate fines and individual imprisonment.

Anti-Money Laundering

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have been derived from legitimate origins or constitute legitimate assets. Money laundering is a particular national security concern because it can be intertwined with financial crime, terrorist financing, and international bribery schemes.

The Bank Secrecy Act ("BSA") is intended to combat money laundering and terrorist financing by requiring banks to establish specific anti-money laundering compliance programs, conduct customer due diligence, screen against Office of Foreign Assets Control ("OFAC") and other government lists, and monitor and report suspicious activity. On January 1, 2021, Congress passed the Anti-Money Laundering Act of 2020 ("AMLA") and the Corporate Transparency Act ("CTA"). These laws expand the types of entities subject to regulation under the BSA, impose new reporting requirements, expand the U.S. government's power to obtain foreign bank records, and create new and increased penalties.

China

The Biden Administration may rebrand the Trump Administration's "China Initiative," but it will continue to focus on countering Chinese national security threats by prosecuting export control and sanctions violations, trade secret theft, hacking, economic espionage, foreign direct investment and supply chain compromises, and covert efforts to influence the American public and policymakers without proper transparency. In fact, on the same day that the Biden Administration issued its anti-corruption national security memorandum, it also issued an ***executive order*** expanding the list of companies with purported links to China's military that are banned from receiving American investment.

Companies with a significant footprint in China are vulnerable to pressure from the Chinese government to act in ways that may be contrary to U.S. regulations. For example, late last year, a China-based executive of the videoconferencing company Zoom was charged criminally for allegedly engaging in a conspiracy with Chinese officials to disrupt video meetings in New York commemorating the Tiananmen Square massacre.[3] It would be reasonable to expect additional, similar types of investigations and charges initiated under the new administration. In addition, companies with operations in China are especially vulnerable to FCPA violations because many seemingly "ordinary" Chinese citizens qualify as foreign officials under the law

due to their employment by a state-owned entity or to their membership in the Communist Party of China. Companies also should expect increasing scrutiny in connection with the Committee on Foreign Investment in the United States ("CFIUS") process where parties have ties to China.[4]

Cybersecurity

At a basic level, companies are expected to protect their data and the data that they collect from their customers, prevent breaches, and respond appropriately should a breach occur. Companies are vulnerable due to the constantly evolving nature of cyber-threats, and because cybersecurity efforts are reliant on human behavior, which can have drastic effects on both the reliability of protective measures, as well as consumer and investor confidence if supply chains or services are interrupted.

There are few formal cybersecurity regulations on the books, although the Biden Administration has signaled the possibility of formal regulations in the near future and is clearly energizing the cyber law enforcement landscape by directing personnel and resources to surge on challenges and threats such as ransomware attacks.[5] In response to strong public outcry regarding ransomware attacks, DOJ flexed its muscles earlier this week by announcing that it had successfully seized $2.3 million in cryptocurrency that had been paid to cyber extortionists last month.[6] One existing area of regulation to be aware of is the Computer Fraud and Abuse Act ("CFAA"), which provides both criminal and civil penalties for accessing a computer system "without authorization" or in a manner "exceeding authorized access."[7] For example, last year, a corporation paid a $10 million penalty as a result of the unauthorized access of a competitor's data, which was facilitated by a prior employee of that company.[8] We can expect to see more investigations in this area, where valuable intellectual property may be at risk due to corporate cyber-enabled espionage.

Sanctions & Export Controls

OFAC administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. Sanctions vary in nature and scope. Some are broad, country-level prohibitions, and others are targeted at specific individuals and entities. The United States also imposes export controls to protect national security interests and promote foreign policy objectives.

Foreign Agents Registration Act

FARA requires certain agents of foreign principals who are engaged in political activities to make periodic public disclosure of their relationship with the foreign principal, as well as activities, receipts and disbursements in support of those activities.

What Companies Can Do to Prepare

Given this expansive enforcement landscape and the Biden Administration's commitment to combatting corruption at home and abroad, there are concrete steps that companies should take now to protect themselves.

First, companies should routinely conduct a risk assessment to identify their exposure in the current climate based on their unique operations. Too often, companies rely on outdated

assessments because of budget or time constraints or a belief that their risk profile has remained largely static. Regular risk assessments are an essential tool to proactively identify new and evolving financial, operational, regulatory, and reputational risks so that they can be evaluated and measures can be implemented to mitigate those with the most risk of significant harm.

Second, companies should ensure that their compliance program is adequately detecting and preventing misconduct. This is especially true as we are coming out of the Covid-19 pandemic, which put a stress on compliance resources and processes. Every company should take a fresh look at their compliance program in light of changes to their operations, be that in the form of funding, remote work arrangements, new technology, or other developments. The government expects companies to have effective compliance programs in place despite the challenges of the past year. When assessing their compliance program, companies should consider how they can align themselves with the government to deter misconduct. Company culture is critical to being able to show that leadership does not turn a blind-eye to risk. Further, the Justice Department has over the past few years put an emphasis on the need to incorporate lessons learned from past misconduct and to implement new processes to prevent repeat offenses.

Third, companies should have a plan in place should misconduct occur. Don't wait until something has gone wrong to develop a plan with counsel for how the company will respond. How a corporation communicates both internally and externally immediately after an incident occurs can be determinative of whether it becomes a subject or target of an investigation. A corporation's strategy when faced with an investigation should be fully informed by an understanding of the government's perspective and how they view the company, and supported by the ability to communicate effectively with the government in order to educate investigators about specialized industries and practices so that conduct can be fairly evaluated.

---

1. The United States Court of Appeals for the Second Circuit held *in United States v. Hoskins*, 902 F.3d 69 (2d Cir. 2018), that the government could not employ theories based on conspiracy or complicity to charge foreign nationals with FCPA violations where a defendant is not otherwise covered by the statute.

2. For example, last month the Justice Department announced charges against the Republic of Chad's former Ambassador to the United States and Canada for soliciting and accepting a $2 million bribe from a Canadian start-up energy company, and conspiring to launder the bribe payment in order to conceal its true nature. *See Charges Unsealed Against Former Chadian Diplomats to the U.S. Charged in Connection with International Bribery and Money Laundering Scheme* (May 24, 2021), ***https://www.justice.gov/opa/pr/charges-unsealed-against-former-chadian-diplomats-us-charged-connection-international-bribery***.

3. *See* Nicole Hong, *Zoom Executive Accused of Disrupting Calls at China's Behest*, N.Y. TIMES, (Updated Feb. 26, 2021), ***https://www.nytimes.com/2020/12/18/technology/zoom-tiananmen-square.html***.

4. CFIUS is an interagency committee authorized to review certain transactions involving foreign investment in the United States and certain real estate transactions by foreign persons, in order to determine the effect of such transactions on the national security of the United

States. Companies engaged in such potential transactions need to be mindful of requirements that may be imposed by the U.S. government before approving such transactions where national security interests are implicated.

5. Bracewell attorneys recently published an ***update*** on this topic.

6. *See Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside* (June 7, 2021), ***https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside***

7. Notably, also on June 3, 2021, the U.S. Supreme Court resolved a circuit split and ruled that an individual does not violate the statute if he has authorization to access a computer system, but uses it for an unauthorized purpose. *Van Buren v. United States,* No. 19-783, -- S.Ct. -- (2021).

8. *See Ticketmaster Pays $10 Million Criminal Fine for Intrusions into Competitor's Computer Systems* (Dec. 30, 2020), ***https://www.justice.gov/usao-edny/pr/ticketmaster-pays-10-million-criminal-fine-intrusions-competitor-s-computer-systems-0***.