Published on *The National Law Review* https://natlawreview.com

# Government Enforcement and Investigations Year-In-Review: The Administration Has Moved Its Pieces into Place

Article By:

Philip J. Bezanson

Kevin D. Collins

Seth D. DuCharme

Matthew G. Nielsen

Anne M. Termine

Jeffery B. Vaden

On Monday, President Biden released the United States Strategy on Countering Corruption, which details how the United States will work "domestically and internationally, with governmental and non-governmental partners, to prevent, limit, and respond to corruption and related crimes." It outlines five pillars of work, which include modernizing efforts to fight corruption, enacting gap-filling legislation to curb illicit finance, increasing federal and state enforcement actions, and leveraging foreign assistance to achieve anti-corruption policy goals. The detailed Strategy is the latest in a series of initiatives and actions in 2021 that have firmly established that the administration is cracking down on corporate crime and ramping up scrutiny on compliance programs across sectors, with a host of measures aimed at filling gaps in anti-corruption, cybersecurity, and ESG enforcement. With respect to civil enforcement, the administration has requested an unprecedented interagency review of existing regulations to tackle new and emerging threats to American business and government. Increased criminal prosecutions are also expected, as the DOJ announced significant changes to its corporate criminal enforcement policies. As enforcement priorities shift in the first year of the new administration, companies should heed Deputy Attorney General Lisa Monaco's stark warning "to actively review their compliance programs to ensure they adequately monitor for and remediate misconduct—or else it's going to cost them down the line."

## Corporate Corruption and Compliance

The Biden administration kicked off its anti-corruption campaign in March when Secretary of State Antony Blinken banned Ihor Kolomoyskyy, a former Ukrainian governor and billionaire accused of "significant corruption," from entering the United States. Foreign Corrupt Practices Act (FCPA)

penalties hit record highs in 2020 and 2019, and are only expected to gain momentum as the Biden administration renews its commitment to fighting corruption both at home and abroad. In a June 2 speech, the Acting Assistant Attorney General Nicholas McQuaid declared that FCPA cases remain a priority and that "there is more to come in 2021."[1]

Also in June, President Biden issued his National Security Memorandum that declared anti-corruption a "core national security interest." The memo initiated a unique interagency review expected to culminate in recommendations as to how the US can modernize intelligence collection, streamline enforcement methods, and build stronger international partnerships to curb global corruption. Although the DOJ and Securities Exchange Commission (SEC) have been the primary enforcers of anti-corruption statutes,[2] Biden's memo called on thirteen additional government agencies to address "all forms of illicit finance in the United States and international financial systems."[3] Notably, this directive closely follows the Anti-Money Laundering Act of 2020 (AMLA), which greatly expanded the government's power to investigate and prosecute financial crime, terrorist financing, and international bribery schemes.

Agencies are expected to release their reports this month, around the same time President Biden will meet with world leaders at the Summit for Democracy, where anti-corruption talks and new Department of Treasury sanctions against individuals engaged in corruption and serious human rights abuses are already on the agenda. While the substance of agency recommendations remains to be seen, they will almost certainly result in an uptick of FCPA and money laundering enforcement actions in the coming months. In addition, the government will likely take advantage of new provisions of the AMLA, which have expanded the government's subpoena power, increased penalties, and improved whistleblower rewards and protections.

## Cybersecurity

In 2021, a growing number of hackers targeted the US economy, including critical infrastructure. At least partly in response to the Colonial Pipelines ransomware attack that shut down the largest pipeline in the US and led to fuel shortages across the East Coast, the Biden administration issued a May 12 Executive Order with the goal of modernizing the federal government's cybersecurity systems. The Order was but the first in a series of White House initiatives this year aimed at securing and defending public systems from cyber criminals.

Observing that "federal action alone is not enough" to combat cyber attacks, on July 28, the President issued a National Security Memorandum that directed agencies to develop voluntary cybersecurity goals for private owners and operators of critical infrastructure and formally established the President's Industrial Control System Cybersecurity (ICS) Initiative. The ICS Initiative is a voluntary, collaborative effort between multiple federal agencies and the critical infrastructure community that has rallied over 150 utilities serving 90 million Americans committing to deploy updated cybersecurity technologies. In August, a meeting between President Biden and private sector leaders similarly resulted in major private-sector companies, including Apple, Google, IBM, Microsoft, and Amazon, committing to initiatives that presumably will improve the security of information and operational technology and the supply chains they support.

Government agencies have also warned of increased enforcement actions against companies that fail to maintain adequate cybersecurity practices and related internal controls.[4] Moreover, in September, the Department of the Treasury's Office of Foreign Asset Control (OFAC) issued an updated advisory warning that ransomware payments to foreign actors subject to US sanctions will result in OFAC enforcement and sanctions up to $20 million per violation.[5] And in October, the DOJ

contributed to the effort with the announcement of its Civil Cyber-Fraud Initiative, which plans to use the False Claims Act to pursue cyber-related fraud by government contractors and grant recipients. In addition to OFAC and DOJ enforcement, the SEC and Federal Trade Commission (FTC) have continued their pursuit of companies that mislead customers with respect to cybersecurity practices in violation of securities laws and the Federal Trade Commission Act.

Although the SEC saw an 18% decrease in total enforcement actions brought in 2021, such a decline is likely attributable to the first year of a new administration seeking to reevaluate its regulatory priorities and re-staff top positions. Now that many of the leadership positions have been filled and strategies have been defined, we can expect increased scrutiny and government enforcement action for companies that fail to implement adequate internal controls, including those that relate to cybersecurity programs. In addition to the patchwork of industry-specific enforcement mechanisms already available to the government, Deputy Attorney General Lisa Monaco in a recent Op-Ed urged Congress to pass comprehensive federal legislation that would create a national standard for private companies to report cyber incidents. Congress has answered the call with multiple bills aimed at increasing cybersecurity spending and breach reporting requirements already on the table for the 117th Session. Accordingly, many corporations have invested in technical, legal, and communications resources that can quickly and accurately identify data breaches to meet expectations for internal and external reporting requirements.

## Cryptocurrency

Cryptocurrencies have become attractive investments for some in the market, as well as a preferred payment method for the distribution of contraband and other illegal goods and services. Although regulatory statutes do not specifically address the cryptocurrency market, the SEC and Commodity Futures Trading Commission (CFTC) have maintained that their respective regulations are flexible enough to cover digital assets. The SEC has stated that the *Howey* test is sufficient to determine if a cryptocurrency is a security; the CFTC has stated that certain cryptocurrencies are commodities subject to, at least, the CFTC's enforcement jurisdiction. The new administration appears committed to these approaches.

The SEC recently has been leading the charge to bring the cryptocurrency community into compliance with existing regulations. Chairman Gary Gensler announced in August that he agrees with his predecessor's view that "almost every ICO … is a security" and is therefore subject to the full gambit of existing securities laws. The SEC brought a total of 16 enforcement actions in the past year against entities that offer unregistered ICOs or make misleading statements to induce the purchase of digital assets.

The CFTC also has been active, bringing a number of cases involving allegations of fraud and manipulation, in addition to failure to register with the agency. In September, the CFTC imposed a $1.25 million penalty against Kraken, one of the largest digital asset exchanges in the US, for offering digital assets without being registered as a futures commission merchant, and in October, fined BitFinex $1.5 million for similar allegations. The CFTC imposed a $41 million fine against another exchange, Tether, for making false or misleading statements about its stablecoin, US Dollar tether token. These cases suggest that the CFTC will not hesitate to assert its enforcement authority over cryptocurrency exchanges that violate the Commodity Exchange Act and CFTC regulations, and will continue to collaborate with the DOJ and other agencies to ensure compliance.[6]

In addition to civil enforcement, the DOJ in October announced the creation of its National Cryptocurrency Enforcement Team (NCET) that will coordinate investigation and enforcement efforts

of various criminal violations involving digital assets. The DOJ has a wide variety of federal charges at its disposal to deal with the misuse of cryptocurrency, including wire fraud, mail fraud, securities fraud, and money laundering, among others.

Despite this extensive arsenal of civil and criminal enforcement mechanisms, multiple government agencies have called on Congress to fill gaps in the existing regulatory framework that continue to widen as the digital currency marketplace grows. The SEC asked Congress for "additional plenary authority to write rules for and attach guardrails to crypto trading and lending." CFTC Acting Chairman Rostin Behnam stated in his nomination hearing before the Senate Agriculture Committee in October that Congress should consider expanding the CFTC's authority to include direct authority to regulate cryptocurrencies. In a November Report, the Department of Treasury similarly urged Congress to pass legislation to ensure that stablecoins are subject to consistent and comprehensive federal oversight. With much at stake, the cryptocurrency industry itself has weighed in on the matter, with Coinbase, the largest cryptocurrency exchange in the US, asking Congress to create a new regulator with sole authority over the emerging marketplace. These suggestions come as Congress explores multiple legislative bills directly impacting the cryptocurrency and blockchain industries in its 117th session. Updated guidance and increased regulation is expected. Until then, the government has encouraged companies to register their digital assets rather than attempt to take advantage of ambiguities in the developing legal landscape.

## Environmental, Social, and Governance

The Biden administration is also prioritizing increased regulation in ESG space, starting with a January 27 Executive Order that placed the climate crisis at the center of US domestic and foreign policy. The Order directed government agencies to "make achieving environmental justice part of their missions by developing programs, policies, and activities to address the disproportionately high and adverse human health, environmental, climate-related and other cumulative impacts on disadvantaged communities, as well as the accompanying economic challenges of such impacts."

Pursuant to this directive, in February, the SEC announced a review of its 11-year-old climate-related disclosure guidance, and in March, announced the creation of its Climate and ESG Task Force, led by the SEC's Deputy Director of Enforcement – a clear signal that updated disclosure requirements and increased enforcement are soon to follow. Consistent with its top down direction, in March, the CFTC established a new Climate Risk Unit to address the role of derivatives in transitioning to a low-carbon economy. The DOJ closely followed suit in June, announcing a rollout of Environmental Justice Teams (EJT), the first of which popped up in the U.S. Attorney's Office for the Eastern District of New York. In a recent conversation with Bracewell, EJT Chief Matt Silverman discussed how his team will prioritize environmental justice in its investigations and enforcement actions. In addition to these various government agencies, the House Committee on Oversight and Reform recently opened an investigation into oil company conduct, alleging that the fossil fuel industry has prevented serious action on climate change through a disinformation campaign similar to that of the tobacco industry decades ago.

A second climate-related Executive Order signed in May ordered the Financial Stability Oversight Counsel to consider issuing a report detailing "plans that member agencies are taking to improve climate-related disclosures . . . and to incorporate climate-related financial risk into regulatory and supervisory practices." One such agency, the Financial Industry Regulatory Authority (FINRA), appears to be taking the lead on diversity, equity, and inclusion (DEI) disclosures, requesting public comments for updates to its DEI rules in June. Just last month, acting FINRA Chair Eileen Murray defended increased government regulation of ESG in an interview with CNBC, calling ESG

“an ecosystem” that will require “regulators, business, and educators” to work together to protect ESG-conscious investors. Murray also applauded the SEC’s decision in August to approve NASDAQ’s new board diversity requirements and hinted that future regulations may reflect a similar comply-or-disclose framework.

The promise of ESG disclosure standards from the SEC, CFTC, and FINRA suggests greater scrutiny and enforcement action on corporations that may toe the line between puffery and misrepresentations in public facing ESG statements. Until then, the new Climate and ESG Task Force has promised to identify and target “material gaps or misstatements in issuers’ disclosures of climate risks under existing rules.”

## Forecast

The themes coming out of the administration in 2021 have been consistent: greater government scrutiny on corporate conduct, with a nose to the ground for signs of corruption across sectors, and a higher standard of scrutiny on representations that tout ESG values as hallmarks of responsible corporate citizenship. Cyber activity, both on the adversarial and regulatory sides, has increased, and can be expected to continue to increase in 2022 as the U.S. government issues a call to arms, which includes a carrot in the form of some level of assistance to private corporations that join hands with the government, and a stick to those that fail to implement adequate security measures and internal controls. In addition, as cryptocurrencies continue to challenge the traditional banking system, the government will try to shore up regulatory schemes with gap filling legislation and aggressive enforcement action, which will likely require updates to companies’ existing AML programs. With respect to criminal investigations, the Deputy Attorney General has instructed her prosecutors to “be bold,” and we can expect them to enthusiastically carry out that mandate. To be well positioned for the year ahead, now is the time for belt tightening in compliance systems and controls.

Meagan C. Maloney also contributed to this article.

1. Nicholas McQuaid, Acting Assistant Attorney General, Dep’t of Justice, Keynote Address at the Foreign Corrupt Practices Act New York (June 2, 2021).

2. In the first corporate FCPA settlement of the year, the SEC and DOJ imposed a $43 million fine against Foster Wheeler for its involvement in a bribery scheme that took place in Brazil. Press Release, U.S. Securities and Exchange Commission, SEC Charges Amec Foster Wheeler Limited With FCPA Violations Related To Brazilian Bribery Scheme (June 25, 2021), https://www.sec.gov/news/press-release/2021-112.

3. In addition to the SEC, the Commodity Futures Trading Commission (CFTC) has also stated an intention to bring enforcement actions alongside the DOJ in cases where its markets are implicated, the first of which resulted in a $95.7 million fine against Vitol Inc. for foreign corruption-related Commodity Exchange Act violations. Press Release, Commodity Futures Trading Commission, CFTC Orders Vitol Inc. to Pay 95.7 Million for Corruption-Based Fraud and Attempted Manipulation (Dec. 3, 2020), https://www.cftc.gov/PressRoom/PressReleases/8326-20.

4. Press Release, U.S. Securities and Exchange Commission, SEC Charges Issuer With Cybersecurity Disclosure Controls Failure (June 15, 2021), https://www.sec.gov/news/press-release/2021-102; Press Release, U.S. Securities and Exchange Commission, SEC Charges Pearson plc for Misleading Investors About Cyber Breach (Aug. 16, 2021), https://www.sec.gov/news/press-release/2021-154.

5. The updated advisory coincided with the OFAC's first-of-its-kind sanction against Russian-owned virtual currency exchange Suex for laundering ransoms from at least eight separate cyber attacks. Press Release, U.S. Dep't of Treasury, Treasury Takes Robust Actions to Counter Ransomware (Sept. 1, 2021) https://home.treasury.gov/news/press-releases/jy0364.

6. Heeding the new administration's calls for interagency collaboration, the CFTC and FinCEN brought concurrent cases against BitMEX for failure to register and failure to implement an adequate AML program, resulting in over $100 million in penalties. Press Release, Commodities Futures Trading Commission, Federal Court Orders BitMEX to Pay $100 Million for Illegally Operating a Cryptocurrency Trading Platform and Anti-Money Laundering Violations (Aug. 10, 2021), https://www.cftc.gov/PressRoom/PressReleases/8412-21.



National Law Review, Volume XI, Number 342