Looking Ahead to 2022:
Significant Trends in White Collar Law & Investigations

whitecollarlawandinvestigations.com
BLOG SERIES
# Table of Contents

**Health Care Enforcement – A Look Ahead** ........................................................................................................... 1  
Lynn Neils

**Anti-Corruption in 2022: A Look Ahead** ............................................................................................................ 3  
Shrutih Tewarie, John Murray, Anthony Mirenda and Howard Weiss

**Criminal Tax Violations: 2022 Enforcement Trends** .......................................................................................... 12  
John Marston and Joanna McDonough

**Office of Massachusetts Attorney General – 2022 Preview** .............................................................................. 14  
Rachel Davidson

**Review of Sanctions and Export Control Developments in 2021 and What to Expect in 2022** .......................... 16  
Shrutih Tewarie, Anthony Mirenda, Luciano Racco, Anna Annino, Daniel Zaleznik and Nick Bergara

**SEC Enforcement in 2022: A Look Ahead** ....................................................................................................... 27  
John Murray and Christian Garcia

**False Claims Act Enforcement in 2022: What to Expect In the Year Ahead** ...................................................... 33  
Neil Austin and Natalie Panariello

**On the Horizon – What’s Next For SEC Enforcement of ESG Priorities** ............................................................ 36  
Matt Miller

**Federal Cryptocurrency Enforcement in 2022** .................................................................................................. 38  
Christopher Hart and Yoni Bard

**Looking at the Landscape of Congressional Investigations in 2022** ............................................................... 42  
Veronica Renzi, Austin A.B. Ownbey, Yoni Bard and Patrick Brennan

www.whitecollarlawandinvestigations.com
Health Care Enforcement – A Look Ahead

This is the first post in this year’s series examining important trends in white collar law and investigations. Join us in the weeks ahead as we provide updates on new developments and emerging trends in a number of white collar spaces. Up next: trends in anti-corruption.

A perennial focus of regulators, health care fraud enforcement remained active in 2021 and is expected to continue in the year ahead. Below we look at some of the drivers of that enforcement activity. Our key takeaways:

- Opioid enforcement actions will remain extremely active in the coming year, including with respect to doctors and pharmacists, not just health care companies and their executives.
- Pandemic-related fraud will continue to be a priority of federal and state enforcement agencies, including investigation regarding the use of pandemic relief funds, fraudulent testing schemes, and false vaccine documentation.
- As the evolving state of the COVID-19 pandemic brings new health services to more Americans, telehealth in particular will be a focus.
- Enforcement agencies will be especially attentive to any actions taken against vulnerable populations, including older adults and recipients of home health services.

Opioids

Continuing with the trend we’ve seen over the last couple years, the U.S. Department of Justice (“DOJ” or “the Department”) remains committed to opioid related enforcement actions. In 2021, the DOJ continued its trend of focusing on doctors and pharmacists, not just companies and executives, involved with the distribution of
opioids. This is not to say that the DOJ is exclusively focused on health care practitioners and pharmacists when it comes to controlled substances, though that is certainly a focus.

The DOJ remains committed to pursuing claims against pharmaceutical companies that they allege marketed opioids with false and misleading statements, paid kickbacks to increase prescriptions, or targeted health care practitioners with a known pattern of problematic prescribing. Although fewer high profile cases in 2021 might have signaled a relaxing of the DOJ’s enforcement actions against companies compared to 2020—which included the department filing suit against Walmart alleging nationwide violations of the Controlled Substance Act and the guilty plea from Purdue Pharma—the DOJ has recently reiterated its commitment to investigating and pursuing claims against health care companies and the department remains active in this space. This includes the Manhattan trial of the former CEO of Rochester Drug Co-Operative Inc. who is charged with conspiracy to violate federal law prohibiting narcotics distribution.

State Attorneys General also remain active in these spheres as evidenced by a recent trial against Teva Pharmaceuticals in New York. In a case brought by the New York Attorney General’s office, Teva was found liable by a New York jury on December 30, 2021, under a public nuisance theory for allegedly fueling the opioid crisis. A damages trial in that case is expected to take place this year. Other state and local actions against opioid manufacturers, distributors, and pharmacies under this theory will continue in 2022 and likely beyond.

**Trials**

Health care saw its fair share of high profile trials in 2021, with Elizabeth Holmes’s multi-month trial ending in a conviction of the former Theranos CEO on three counts of wire fraud and one count of conspiracy. Although the 12-member jury cleared Holmes on three counts of fraud and one conspiracy count related to defrauding patients, the verdict carries the possibility of significant jail time for the former executive and serves as a cautionary tale for health care executives. Holmes’s former boyfriend and former Theranos Chief Operating Officer Samesh Balwani is set to face his own charges before a jury in February.

**COVID-19**

COVID-19 related enforcement efforts continued to be a priority for the DOJ. With increased vaccine supply and the rise of vaccine requirements in various settings, the DOJ saw increased fraud related to the vaccine and brought numerous actions related to fraudulent COVID-19 vaccine cards.

The DOJ also remains active in investigations related to COVID-19 relief funds and COVID-19 testing schemes that misused information and samples obtained at COVID-19 testing sites to submit claims to Medicare for medically unnecessary, and often expensive, laboratory tests.

We can expect this space to remain active, as the Department has expressed its continuing commitment to combatting pandemic-era fraud. The Attorney General created the COVID-19 Fraud Enforcement Task Force in 2021, which is a special task force formed to coordinate resources and information across the Department and other governmental agencies to better identify and prevent fraud. Followers can expect continued coordination efforts as federal and state authorities are continuing to coordinate on strategic enforcement, with organized meetings to discuss various fraud schemes related to the pandemic identified in different states.
**Telehealth**

One of the DOJ’s focuses coming out of the COVID-19 pandemic is on telehealth providers, in particular CMS regulations put in place during the COVID-19 pandemic that broadened telemedicine options for Medicare beneficiaries. A [February 2021 speech](#) by the then-acting Assistant Attorney General Brian M. Boynton predicted telehealth schemes would be a continued focus of the Civil Division of the DOJ. That prediction bore true with telemedicine fraud schemes amounting to some of the largest fraud enforcement actions in 2021. Notably, a September 17, 2021 enforcement action [press release](#) announced criminal charges against 138 defendants across 31 federal districts in the United States amounting to approximately $1.4 billion dollars in losses. Of the $1.4 billion in total losses, fraud schemes related to telemedicine amounted to $1.1 billion of those losses. In [one of the largest Medicare fraud schemes ever charged](#) by the Justice Department, a Newark, New Jersey grand jury indicted a Florida owner of multiple telemedicine companies on allegations of orchestrating a health care fraud scheme that involved $784 million of false and fraudulent claims to Medicare.

These enforcement efforts demonstrate that telehealth, as a new and evolving space for health care, is an area the government continues to scrutinize closely. Telehealth providers should be vigilant in their compliance efforts and consider investing in, and developing, a robust compliance program.

**Vulnerable Populations**

2021 also saw a focus on fraud schemes related to older adults and vulnerable populations in the health care space. Enforcement actions against hospice fraud and home health care fraud schemes were particularly active last year. Additionally, and related to the DOJ’s opioid enforcement efforts, the DOJ focused attention on fraud related to substance abuse clinics and treatment facilities.

This year we expect this trend to continue, as evidenced in a [December 2021 speech](#) by the Associate Attorney General Vanita Gupta reiterating the Department’s commitment to combating health care fraud and abuses against elder adults.

---

**Anti-Corruption in 2022: A Look Ahead**

Posted on [February 14th, 2022](#) by Shruti Tewarie, John Murray, Anthony Mirenda and Howard Weiss

*This is the second post in this year’s series examining important trends and new development in white collar law and investigations. Our previous post discussed health care enforcement. Up next: trends in tax enforcement.*

As the Biden administration moves into its second year, we anticipate both an increase in U.S. anti-corruption enforcement activity, and a broader, whole-of-government approach that seeks to encourage and reward international partners for their efforts in combating corruption. Across the globe, key actors continue to push
for increasing transparency, setting rising expectations for the adoption of anti-corruption best practices and for efforts to hold corrupt actors accountable. As we discuss below, we expect that the U.S. Department of Justice (“DOJ”) and Securities and Exchange Commission (“SEC”), along with law enforcement agencies outside the U.S., will follow suit. Our key takeaways:

- The Biden administration has singled out anticorruption as a “core national security interest” and “core domestic and foreign policy priority,” signaling that the administration will redouble its efforts on this front.
- Recommendations from the OECD will heighten the pressure on nations to ramp up their efforts to fight corruption within their own borders.
- The U.S. has significantly expanded its legislative and regulatory arsenal to increase corporate transparency and combat money laundering.
- U.S. enforcement actions will likely increase in 2022 as investigations in the pipeline begin to bear fruit and U.S. law enforcement agencies increasingly coordinate their investigations with their counterparts abroad.
- Reflecting similar trends globally, the EU, France, the United Kingdom, and China also implemented major enhancements to their anti-corruption regimes.

**Major U.S. Policy Initiative**

In December 2021, the Biden administration made a major policy announcement in its release of the U.S. Strategy on Countering Corruption, which takes an aggressive and purposeful stance, describing combatting corruption as a “core domestic and foreign policy priority” and a “core national security interest.” The administration also clarified that its “new approach” consists of five pillars: (1) expanding the commitment of U.S. resources; (2) curbing illicit finance; (3) holding corrupt actors accountable; (4) obtaining multilateral cooperation; and, (5) improving diplomatic engagement and foreign assistance. While each pillar contains familiar elements, by bringing them together into a thematic whole and presenting them as a national security priority, the administration has ramped up the level of commitment and attention to this issue.

The Strategy sets forth a variety of steps the administration will take to effectuate the five pillars. For one, it is committed to aggressively implementing and expanding the suite of U.S. anti-corruption laws. For example, it has pledged to prioritize rulemaking under the Corporate Transparency Act (“CTA”), passed last year, which imposes reporting requirements on beneficial owners of certain companies in order to hinder the ability to use shell companies to hide and launder the proceeds of corruption. The Strategy also includes additional transparency-focused regulations, reaching corruption-sensitive areas such as government procurement transactions and real estate transactions. Lastly, the Strategy notes the administration’s aim of working with Congress to expressly criminalize “demand-side” bribery – i.e., the solicitation of bribes by foreign public officials, as distinguished from the payment of bribes to them – a measure that Congress has long debated but thus far has declined to enact. (We discuss the CTA, as well as proposed legislation in Congress that would prohibit demand-side bribery, and other legislation, below.)

The administration also intends to place particular weight on anti-corruption as a factor in its decisions about how and where to deploy U.S. foreign aid. It recently established a task force at the U.S. Agency for International Development focused on this issue, currently seeks to create a similar task force at the Department of Commerce, and is launching an interagency Democracies Against Safe Havens Initiative to coordinate transnational law enforcement, sanctions, and other anti-corruption efforts. Moreover, the Strategy explicitly commits the administration to “vigorously pursue the enforcement of foreign bribery cases through the FCPA” and bring other “aggressive enforcement action.”
Updated OECD Recommendation for Further Combatting Bribery of Foreign Public Officials

Anti-corruption efforts are the forefront of other nations’ agendas in 2021 as well. Biden’s Strategy announcement came on the heels of the 2021 Recommendation for Further Combating Bribery of Public Officials in International Business Transactions (“2021 Recommendation”) by the Organization of Economic Cooperation and Development (“OECD”). Updating its last Recommendation from 2009, the OECD Recommendation presents an international consensus on issues of corruption and delineates a strategy for moving forward.

The Recommendation consists of four key components. First, the OECD instructs countries to focus on the demand-side of corrupt schemes. Rather than push nations such as the United States to expand their extra-territorial exercise of jurisdiction (a step that legislation currently pending in Congress, discussed below, would take), the OECD urges those nations whose officials solicit bribes to raise awareness of the risks of bribery, assist in the coordinated investigation of bribery solicitation, and prosecute bribery schemes domestically where necessary. In doing so, the OECD is attempting to balance the long-standing tension between what historically has been seen as inadequate local efforts to combat corruption, and the ramifications of enforcement from abroad by the United States and other aggressive external enforcers.

The three other central components of the 2021 Recommendation incorporate longstanding U.S. tools that have been less of a focus elsewhere. For example, the OECD asks that countries leverage more non-trial mechanisms, such as deferred prosecution agreements, on the rationale that incentivizing a company’s voluntary self-disclosure, cooperation with law enforcement, and remediation will aid in exposing corrupt practices, while holding companies accountable for that misconduct. The OECD also recognizes the importance of “strong and effective legal and institutional frameworks” to protect whistleblowers who report suspected acts of bribery. Finally, the OECD’s Recommendation emphasizes the importance of international cooperation, explaining that multijurisdictional cases call for a proactive approach to sharing information and evidence, and direct coordination in investigating and prosecuting corrupt actors.

The OECD also expanded its “good practice” guidance by adding more recommendations concerning internal controls, audits, and compliance incentives for companies. We expect this guidance and the OECD’s Recommendation to influence anti-corruption enforcement globally as nations continue to ramp up and coordinate their anti-corruption efforts.

The Anti-Money Laundering Act of 2020

The Anti-Money Laundering Act of 2020 (“AML”) became effective January 1, 2021 and will continue being implemented in 2022. The AML, seen by many as the most significant U.S. anti-money laundering reform in a generation, will significantly increase the tools the federal government has at its disposal in fighting corruption.

First, the CTA—one part of the AML—will allow the Federal government to compile information on the true beneficial owners of certain companies into a database that will be shared across government agencies. In December, FinCEN issued a notice of proposed rulemaking for the first of three regulations implementing the CTA. This first proposed rule defines which companies must file reports, what specific information will be included, and when each report is due. Although the CTA now limits who ultimately will be able to access the database, this law is the first step towards bringing the United States more in line with corporate disclosure requirements in other countries, and its implementation will inevitably put pressure on Congress to expand such access. For a more detailed overview of the CTA, see our prior client alert here.
The AML also expanded federal authority to subpoena non-U.S. bank records. The new law allows the government to subpoena not only any records relating to a correspondent account that a foreign bank chooses to maintain in the United States, but also permits a subpoena of accounts wholly unrelated to the non-U.S. bank’s correspondent account that are maintained outside of the United States. Moreover, the AML expressly prohibits the bank from disclosing the existence or contents of the subpoena to the bank’s account-holder. Lastly, Congress has reduced the importance of respecting compliance with non-U.S. confidentiality or secrecy laws, explaining that the non-U.S. bank may not quash or modify the subpoena solely based on the assertion that compliance would conflict with obligations under such non-U.S. laws.

Additionally, the AML has expanded whistleblower protection and awards. The law was modeled on Dodd-Frank, but has added protections for internal whistleblowers. The AML now allows for whistleblowers to obtain up to 30% of monetary sanctions awarded and removes any discretion to deny a reward if the whistleblower meets certain requirements.

One area that appears less likely than others to be the focus of rulemaking under the AML in the near term is the high-end art market, following a recent study by the U.S. Treasury Department. The study, which was mandated by the AML, concluded that while high-value art poses some risk of money laundering, there is limited evidence of terrorist financing risk. To address those risks, the study recommends that Treasury consider encouraging participants in the art market to share information, updating guidance and training for law enforcement, using recordkeeping authority to support information collection and enhanced due diligence, and applying anti-money laundering and counter-terrorism financing obligations on certain market participants. The latter two recommendations may be the subject of additional rulemaking at some point, but in view of the study, do not appear to be immediate priorities.

**U.S. Enforcement Trends in 2021 and Looking Forward in 2022**

*Policy Statements from DOJ & SEC*

The DOJ has reverted to certain Obama-era policies, raising the bar for corporate cooperation credit and imposing harsher consequences for corporate crime. First, in an October 2021 speech, Deputy Attorney General Lisa Monaco announced that the DOJ has restored prior guidance under the 2015 “Yates Memo” (named after then-Deputy Attorney General Sally Yates), which required companies to provide “all relevant facts about the individuals involved in corporate misconduct” in order to receive cooperation credit. In 2018, the DOJ under the Trump administration modified this policy to require only the identification of individuals “substantially involved in or responsible for the criminal conduct,” rather than more peripherally relevant employees. Monaco explained that the prior policy “afford[ed] companies too much discretion” in their disclosures to the government and hampered efforts to ensure accountability to individuals.

Second, Monaco reversed course on policies that tended to reduce the cost of corporate resolutions for companies. In 2018, the DOJ issued guidance that de-emphasized corporate monitorships. In particular, the guidance instructed prosecutors to reserve corporate monitors for companies that fail to demonstrate that their compliance programs are “effective and appropriately resourced at the time of resolution[].” This will likely change in 2022, however, as Monaco made clear in her speech that “[t]o the extent that prior Justice Department guidance suggested that monitorships are disfavored or are the exception, I am rescinding that guidance.” Monaco also introduced new guidance that will require prosecutors in Foreign Corrupt Practices Act (“FCPA”) cases to consider all of a company’s previous violations, whether or not related to bribery, in determining charges and evaluating potential resolutions. Following Monaco’s speech, DOJ released a memorandum summarizing these changes to DOJ’s corporate criminal enforcement policy.
Soon after the DOJ announced these policy changes, Gary Gensler, confirmed as the SEC Chairman last year, remarked that “these changes are broadly consistent with [his] view of how to handle corporate offenders.” Thus, companies under investigation should be prepared to face greater hurdles to obtaining cooperation credit from both agencies.

Potential Legislation

The Foreign Extortion Prevention Act (“FEPA”) is one of seven bills contained in the Counter Kleptocracy Act, which was introduced in the House of Representatives in September 2021 with bipartisan support. FEPA aims to criminalize foreign officials who demand or accept bribes, filling in the gaps in the FCPA which currently only criminalizes the bribe-giver. While creative prosecutors have long used other charges, such as money laundering and the Travel Act, to go after demand-side actors, FEPA would establish a more direct, FCPA-like path.

The fate of FEPA is uncertain, as Congress considers the jurisdictional and due-process issues inherent in the extra-territorial application of U.S. laws. Even more complex are the diplomatic, foreign policy and national security issues that often arise when considering the prosecution of a foreign official. As discussed above, the OECD Recommendation that nations whose officials solicit bribes invest greater resources into internal anti-corruption efforts might lessen the pressure on the United States to prosecute foreign officials for demand-side bribery.

The other six bills in the Counter Kleptocracy Act contain a variety of possible anti-corruption advancements: (i) a bill providing for a report including a tiered ranking of countries based upon each country’s anti-corruption efforts; (ii) a bill authorizing visa bans against foreign persons engaging in corruption against a U.S. person (the “Foreign Corruption Accountability Act”); (iii) a bill creating a database of investor visa denials to be shared with other countries to prevent the abuse of investor visas by corrupt foreign officials; (iv) a bill providing for a website accounting for the amount of money “stolen from the people” of each country due to foreign corruption that has been recovered by the United States (the “Justice for Victims of Kleptocracy Act”); (v) a bill limiting the confidentiality of the denial of a visa or permit based upon the foreign national’s involvement in corruption or human rights abuse; and (vi) a bill addressing a variety of efforts to counter foreign governments’ abuse of INTERPOL records and procedures to pursue and harass political opponents.

On February 4, 2022, the House of Representatives passed the America COMPETES Act, which includes four anti-corruption bills. One bill, the Countering Russian and Other Overseas Kleptocracy Act (the CROOK Act), aligns with one of Biden’s five pillars—improving diplomatic engagement and foreign assistance—by creating an “Anti-Corruption Action Fund” to be used to support foreign states in their anti-corruption efforts. Notably, the Fund would be financed through $5 million “prevention payment[s]” required to be made by any person who resolves a FCPA charge for greater than $50 million. The COMPETES Act would also strengthen the Global Magnitsky Human Rights Accountability Act, and includes the Foreign Corruption Accountability Act and the Justice for Victims of Kleptocracy Act, both of which, as noted, were also contained in the above-mentioned Counter Kleptocracy Act.

Additionally, the ENABLERS Act was introduced on October 6, 2021 with bipartisan support. The act would expand the Bank Secrecy Act by imposing customer due diligence requirements on gatekeepers such as accountants, investment advisers, lawyers and art dealers. In particular, these gatekeepers would be required to report suspicious transactions, establish anti-money laundering programs, implement due diligence policies, procedures, and controls, and identify and verify their account holders. This bill was precipitated by pressure mounting in the wake of the Pandora Papers, a leak of almost twelve million documents revealing...
the movement of proceeds of corruption, which placed the United States front-and-center as a haven for corrupt proceeds.

Although the outcome of these bills remains uncertain, they fit into Congress’s recent efforts to more closely align AML enforcement with initiatives in other parts of the world.

**DOJ Corporate Enforcement Actions Likely to Increase in 2022**

The number of DOJ corporate enforcement actions (only three corporate resolutions) was lower in 2021 as compared to previous years. A DOJ official recently stated that companies should not expect 2022 to follow this trend, however, as there is a “very robust pipeline” of current investigations.

There are some useful lessons to take from the three corporate resolutions (involving two global banking institutions and one financial services institution). For one, these cases provide examples of large multinational corporations that did not voluntarily self-disclose but received at least partial cooperation credit for their efforts once faced with an investigation.

Also notable was the difference in cooperation credit received. One company only received reduced credit for cooperation because it significantly delayed producing key evidence. In comparison, the others received full cooperation credit for efforts including (i) making prompt and extensive document productions to the government; (ii) facilitating interviews of foreign-based employees; (iii) providing regular updates of the company’s internal investigation to the government; and (iv) making factual presentations and highlighting key facts and documents to the government. The DOJ also credited these companies for engaging in remedial measures during the investigation, including enhancing compliance procedures, disciplining employees involved in the corruption, and providing additional compliance training.

All three companies were required to update their compliance systems in line with the requirements outlined by the DOJ. These detailed frameworks provide a window into the DOJ’s current expectations for a satisfactory compliance program, including:

- a clear and visible anti-corruption policy, addressing issues such as political contributions, facilitation payments, risk-based procedures for ongoing customer due diligence, and identification and reporting of suspicious activity;
- directors and senior management providing a strong, explicit, and visible commitment to the anti-corruption policies and at least one senior executive being assigned implementation and oversight responsibilities;
- due diligence requirements for working with third-party business partners as well as for mergers and acquisitions;
- internal controls to ensure fair and accurate books, records and accounts;
- a system for internal and confidential reporting of violations;
- sufficient employee training;
- effective enforcement and discipline; and
- periodic testing and updating of the program as appropriate.

**Increasing Prosecutions of Individuals**

In line with DOJ and SEC emphasis on individual accountability, 2021 saw an increase in the prosecutions of individuals, including government officials, diplomats, executives at state-owned enterprises, and others.
involved in corruption schemes. For example: the SEC obtained a final judgment against a former executive of a foreign-based subsidiary of a U.S. bank holding company for his role in helping his client bribe Ghanaian government officials for their approval of electrical power plant project. DOJ has maintained its long-standing focus on activity in South America and Central America, including:

- sentencing an Ecuadorian businessman as a conspirator in a bribery scheme involving PetroEcuador, a state-owned oil company (the latest in a series of prosecutions involving PetroEcuador officials and others);
- charging two Ecuadorian citizens for their involvement in a bribery and money laundering scheme involving Ecuador’s public police pension fund;
- prosecuting a dual U.S.-Venezuelan citizen and former official at Citgo, a Houston-based subsidiary of Venezuela’s state-owned energy company Petróleos de Venezuela S.A. (PDVSA), for accepting bribes and laundering bribe proceeds (to date, the DOJ has announced charges against 28 individuals, 22 of whom have pled guilty, for conduct associated with bribery schemes involving PDVSA); and
- charging multiple bank executives for diverting funds from a publicly traded company into a secret slush fund used to bribe Brazilian government officials.

Further, DOJ and the Department of Homeland Security (“DHS”) created a joint task force in 2021 to focus investigative and prosecutorial resources on current corruption and human trafficking systems in Mexico, Guatemala, El Salvador, and Honduras. These enforcement efforts parallel the State Department’s diplomatic efforts to provide support to anti-corruption work in this region.

While Congress continues to debate whether to pass legislation expressly targeting demand-side bribery, DOJ prosecutors continue to use money laundering conspiracy and other charges to reach former foreign government officials, former diplomats, and foreign nationals. For example, the DOJ used the federal money laundering statute to charge a former Bolivian minister and his chief of staff for obtaining bribes paid by a U.S. company in exchange for a $5.6 million contract from the Bolivian Ministry of Defense, where the payments were laundered through bank accounts in Florida. Similarly, two former diplomats, including a former Ambassador, from the Republic of Chad were charged with a money laundering conspiracy based on their alleged solicitation and receipt of a bribe related to procurement of oil rights in Chad.

International Enforcement Trends Looking Forward in 2022

France

At the end of 2020, the French parliament asked members of the French National Assembly to assess the impact of Sapin II, France’s anti-corruption law. That effort resulted in the introduction of a new bill in the French parliament in October 2021 that proposes various changes to strengthen Sapin II. These changes include expanding the reach of Sapin II’s compliance obligations to apply to French subsidiaries, regardless of where the parent company is incorporated, which are part of a group exceeding the cumulative thresholds of 500 employees and €100 million in turnover at the group level. In other words, French subsidiaries of large companies, including U.S. companies, could soon be subject to the requirements of Sapin II. This bill also broadens the scope of criminal liability, as it would include liability for a failure to supervise an employee committing a criminal offense. Further, the new bill introduces a number of other changes to encourage companies to enter into a Convention judiciaire d’intérêt public ("CJIP"), France’s equivalent of a deferred prosecution agreement.

The OECD issued a report in December 2021, reviewing and commending many of France’s recent legislative reforms. Yet the OECD was simultaneously skeptical of one aspect of this proposed bill, which the OECD
described as a “proposed overhaul” of France’s anti-corruption agency, the AFA. It is unclear what impact the OECD’s concerns may have, but the OECD’s report and continuing review of France’s anti-corruption efforts will likely put pressure on France to push forward on implementing the anti-corruption changes outlined above.

United Kingdom

In April 2021, the U.K. Government implemented a new sanctions regime aimed specifically at corruption. The Global Anti-Corruption Sanctions Regulations 2021 (“Regulations”) follow and complement the U.K.’s Global Human Rights Sanctions Regulations 2020. The Regulations are a component of the U.K. Government’s Anti-Corruption Strategy 2017-2022, as well as the Government’s broader effort to develop post-Brexit sanctions that are untethered to the EU’s sanctions regime.

The new regime, which follows an approach similar to the U.S. Global Magnitsky Program, allows for sanctions against individuals and entities that the Foreign Secretary has “reasonable grounds” to suspect are involved in “serious corruption.” On the same day that the Regulations became effective, the Foreign Secretary announced that sanctions had been imposed on 22 individuals involved in “notorious corruption” in Russia, South Africa, South Sudan and Latin America, and several more designations were announced during the year. The Regulations further strengthen already robust U.S.-U.K. cooperation. In announcing the new regime, the Foreign Office made clear that the Regulations “are being taken partly in tandem with the US,” while the U.S. Treasury Department issued a press release enthusiastically welcoming them.

On the enforcement front, the Serious Fraud Office (“SFO”), the U.K.’s chief prosecutor of foreign corruption, had a challenging year. As we reported last year, in February 2021, the U.K. Supreme Court limited the extra-territorial application of evidence-gathering sections of the Criminal Justice Act of 1987, ruling that the SFO cannot compel a foreign company that does not have a registered office in the U.K. and has never carried out business in the U.K. to produce documents located outside the U.K.

Over the past few years, the SFO has moved increasingly towards the U.S. practice of corporate bribery resolutions through Deferred Prosecution Agreements (“DPAs”) and cooperation by key individuals. While this approach has yielded some notable successes with respect to companies, it has engendered criticism from some quarters that it has not been accompanied by successful prosecution of culpable individuals.

The SFO suffered some setbacks in this area last year. Most notably, in December, the Court of Appeal, citing disclosure failures by the SFO, reversed the conviction of a former executive of energy company Unaoil for conspiring to bribe Iraqi officials to obtain oil contracts, leading the U.K.’s attorney general to open an investigation into the SFO’s handling of the case. Especially in light of the resulting pressure on the agency, we expect that the SFO will place particular emphasis on holding individuals accountable in 2022.

China

Like the OECD and the U.S., China announced a significant anti-corruption policy initiative this past year, which we expect will shape the anti-corruption landscape in China in the years to come. The “Opinion on Furthering the Investigation of Giving and Taking Bribes” was jointly promulgated by six Chinese government agencies in September 2021. This opinion outlines the government’s intention to focus on bribe-givers as well as bribe-takers in its anti-bribery efforts. Previously, the government had focused on the recipients of bribes but had prosecuted bribe-givers less frequently. Relatedly, the Opinion mentions the possible creation of a blacklist as a sanction for companies providing bribes in China. In addition, China introduced a non-prosecution
compliance mechanism for entities facing criminal bribery charges, creating a pathway for companies to resolve charges and improve compliance.

Although seemingly tightening its internal anti-corruption enforcement, China has also introduced laws that will create more difficulties for other nations seeking to engage in cross-border investigations. In particular, China’s Data Security Law went into effect on September 1, 2021, providing that data may not be provided to other governmental law enforcement agencies without Chinese government approval. This will both slow down as well as restrict the flow of information to other nations for purposes of investigating and combatting corruption.

EU Prosecutor

The European Union last year added a new weapon to its anti-corruption arsenal with the formation of the European Public Prosecutors Office (“EPPO”). The EPPO is charged with pursuing misuse of EU funds, including corruption involved in EU subsidies or contracts, which have often been directed to businesses connected to local officials. The creation of the EPPO, headed by a former anti-corruption prosecutor from Romania, is significant in that the EU previously depended on member states to prosecute such misconduct, a less than optimal approach because states often failed to pursue these cases. Though several member states have opted out of the EPPO’s jurisdiction, including Denmark, Ireland, Poland, and Hungary, the EPPO appears to be off to a vigorous start. Its anticorruption matters to date include, among others, investigations of a Croatian mayor who allegedly accepted bribes in awarding a contract for a recycling center, and a former Czech prime minister in connection with tens of millions of euros in subsidies paid to companies he formerly owned. Given similar patterns in other EU countries – particularly in Eastern Europe – we expect to see continued EPPO activity in this space during 2022.

World Bank

In October 2021, the World Bank Group issued its Sanctions System annual report. The report reflected a downtick in investigations and referrals by the Bank’s Integrity Vice Presidency (“INT”), which received significantly more complaints (4,311 compared to 2,598 in fiscal 2020), but opened fewer preliminary investigations (347 compared to 429 in fiscal 2020), leading to the opening of 40 full investigations. INT also referred significantly fewer cases and settlements to the Office of Suspension and Debarment (17 and 18, respectively, versus 26 and 22 in fiscal 2020). Consistent with prior years, approximately 21 percent of INT’s referrals involved corruption, and of the 54 debarments imposed, nine were based at least in part on corrupt activity. The Bank also recognized 92 cross-debarments based on debarments by other leading multi-national development banks. INT attributed the relatively slow pace of investigative activity to travel restrictions and other limitations resulting from the COVID-19 pandemic. We anticipate the number of investigations and referrals to rebound towards previous levels as the pandemic ebbs.
Criminal Tax Violations: 2022 Enforcement Trends

Posted on February 16th, 2022 by John Marston and Joanna McDonough

This is the third post in this year’s series examining important trends in white collar law and investigations. Our previous post discussed trends in anti-corruption. Up next: State AG enforcement trends.

- While the volume of IRS enforcement actions has waned, it may soon increase.
- Even at current relatively low audit and investigation levels, the IRS remains aggressive in the cases it does pursue.
- The IRS is focusing efforts on cryptocurrency matters, international investigations, and Covid-19 fraud.
- But the IRS also continues to pursue cases in many traditional areas, where a pre-filing holistic review of issues is the best approach.

Tax season is here — what better time to discuss trends in federal tax investigations?

In recent years, the overall volume of IRS enforcement activity has decreased, both in civil audits and criminal investigations (see links to recent IRS annual Data Books here, and IRS Criminal Investigation (“IRS-CI”) Annual Reports here). Despite years of calling for additional budgets and staffing, and the fact that IRS enforcement is generally a money-making enterprise for the government, meaningful increases in enforcement personnel and activities have not occurred. The recent Build Back Better bill included an $80 billion budget boost for the IRS over the next decade, but that bill has gone notoriously nowhere. Still, politicians continue to tout the benefits of a stronger IRS. While watching IRS enforcement get tossed around on Capitol Hill might be mildly entertaining (or incredibly frightful), it is important to remember decreased enforcement does not equate to zero enforcement, and as always, IRS is following the money.

In terms of white collar crime enforcement, the focus of our blog series, the IRS remains a significant and leading government agency. IRS-CI is the federal agency responsible for investigating and recommending prosecution of criminal tax violations and other related financial crimes to the Department of Justice. It is the only agency that dedicates one-hundred percent of its time to financial investigations. According to the IRS-CI’s 2021 Annual Report (“2021 Annual Report”), this past year IRS-CI spent 72% of its time investigating tax-specific crimes (including, but not limited to, the “exponentially” growing category of cybercrimes), 15.4% of its time investigating non-tax financial crimes such as money laundering (“tax fraud in progress”), and 11.2% of its time on narcotics-related cases through participation in the Organized Crime Drug Enforcement Task Force.

Since October 2020, IRS-CI Chief Jim Lee, a 25-year veteran of the organization, has headed the division. Mr. Lee clearly supports IRS-CI sticking to its core mission. While the heavy focus on convicting people and seeing them sent to jail is sometimes hard to stomach for the defense-minded among us, IRS-CI continues to tout its nearly 90% conviction rate and has emphasized that the consequence of willful non-compliance is jail time, the average being about 43 months this past year. No doubt IRS-CI’s reputation remains strong, and past performance certainly means taxpayers must take future dealings with IRS-CI seriously.

Going forward, IRS-CI under Mr. Lee has emphasized the following areas of focus in 2022:
**Cryptocurrency**

In FY2021, IRS-CI seized $3.5 billion in cryptocurrency, comprising 93% of IRS-CI’s seizures. This included a $1 billion seizure of previously undetected bitcoin transactions executed by Silk Road, which were the proceeds of unlawful activity (Silk Road’s founder, Ross Ulbricht, was convicted in 2015 of conspiracy to distribute narcotics and money laundering). Just last week in an investigation led by IRS-CI, two individuals were arrested for conspiring to launder cryptocurrency that was stolen in a 2016 hack of Bitfinex, a virtual currency exchange. This case also involved the largest-ever financial seizure by DOJ, coming in at $3.6 billion. IRS-CI’s message around cryptocurrency is this: it’s not as anonymous as criminals think.

The focus on cryptocurrencies follows IRS-CI’s growing focus on its cybercrimes program more generally. Knowledge of cryptocurrency, blockchain and open-source intelligence (OSINT) technologies (in addition to other internet and internet-based technologies) is a significant focus in IRS-CI’s attempts to unravel complex cyber-financial criminal schemes. With that in mind, IRS-CI plans to launch an Advanced Collaboration & Data Center (“ACDC”) in the Northern Virginia area later this year. The focus of the center will be to bring together data, technology, and specialized personnel from across Treasury and government to work on high impact solutions to protect the integrity of the tax and financial systems. While IRS-CI has been doing this work on a smaller scale for the past five years, the plan is that the ACDC will give all agents across the country who encounter cyber issues in their investigations the expertise and resources to move cases forward.

**International Partnerships**

IRS-CI’s presence reaches far beyond the United States, and increasingly so. Currently, IRS-CI has 22 attachés in 11 countries covering all of the major regions of the world. In addition to its own resources, IRS-CI relies heavily on international partnerships. For example, in the press release this week related to the arrests/seizures stemming from the Bitfinex hack, the government noted that police in Germany provided important assistance. This past year, IRS-CI marked the third anniversary of the establishment of the Joint Chiefs of Global Tax Enforcement, an international group of tax organizations from five countries (including the US, UK, Canada, Australia, and the Netherlands) known as the “J5.” The J5 combats tax crime through collaboration, information-sharing, and enforcement operations, and undoubtedly will be a significant factor in enforcement actions to come.

**Covid-19 Related Fraud**

Covid-19 related fraud continues to occur, and will be a focus of IRS enforcement. In FY2021, IRS-CI initiated over 300 Covid-19 related cases. Most of these cases involve money laundering in connection with the Paycheck Protection Program (“PPP”), but IRS-CI has also seen fraud in connection with other Covid-19 relief programs, including the Economic Injury Disaster Loan program, unemployment insurance benefits through the CARES Act, and most recently the Childcare Tax Credit. Mr. Lee emphasized that the pace of these investigations is critically important to stop this type fraud in its tracks.

While the areas outlined above are clearly at the cutting edge of IRS-CI’s efforts, it is important to remember that the IRS remains incredibly active in many other areas as well. For example, conservation easement cases continue to surge in both civil and CI matters, and even despite recent losses in some of those cases (see here and here), IRS does not appear close to backing down. Traditional examinations and enforcement actions against high-income individuals and large companies will always be a focus for the IRS. In those matters, and many others, the best defense is typically a pre-filing holistic and thorough consideration not just of the letter
of the law, but also the IRS’s many available tactics to re-interpret a person’s or company’s business and financial decisions. Banking on skating past the IRS’s decreased audit/investigation presence is not a viable plan, because when they do take a shot, as Mr. Lee makes clear, they do everything they can not to miss.

Office of the Massachusetts Attorney General – 2022 Preview

Posted on February 22nd, 2022 by Rachel Davidson

This is the fourth post in this year’s series examining important trends in white collar law and investigations. Our previous post discussed trends in tax enforcement. Up next: trends in sanctions & export controls enforcement.

2022 is shaping up to be an interesting year for the Office of the Massachusetts Attorney General. It marks Maura Healey’s final year as AG as she gears up for her run for governor. Of course, her departure means that the Commonwealth will have a new AG in 2023. This post previews what we expect to be AG Healey’s priorities in the final year of her tenure, namely:

- Active enforcement and settlement of healthcare fraud;
- Commitment to climate change, including the AG’s suit against Exxon Mobil; and,
- Creation of the Conviction Integrity Unit.

Healthcare Fraud

Historically, Healey’s Office has devoted significant resources to the Medicaid Fraud Unit. 2021 was no different. The Medicaid Fraud Division recovered more than $55 million last year, securing 22 civil settlements with various entities, including home health agencies, substance abuse treatment facilities, adult day health centers, adult foster care providers, skilled nursing facilities, and dental practices. This strong success rate suggests 2022 will continue the pattern of healthcare fraud enforcement.

In addition, with COVID still looming large in the Commonwealth, we expect pandemic enforcement to continue, with an increased focus on identity theft, the False Claims Act, and fraud with respect to COVID-treatment and products. For example, near the end of 2021, Healey sued School Health Corporation under the Massachusetts False Claims Act for allegedly misleading Massachusetts school districts into purchasing more than $100,000 worth of fake and ineffective hand sanitizer. (This suit follows a $550,000 settlement in November 2020 with Federal Resources Supply Company for the same conduct used against the Massachusetts Bay Transportation Authority.) As time passes revealing similarly fraudulent behavior and with COVID still on the forefront of the public’s mind, we expect to see this and like cases brought by the AG’s office.
Climate Change and the Environment

Climate change and the environment more broadly have long been a priority of Healey. 2021 continued the AG’s focus in this space. For example, in September 2021, Healey settled with a New Bedford-based school bus company over allegations that its drivers excessively idled their buses at several schools. In conjunction with the settlement, Healey also launched the Clean Air Initiative, an initiative focused on tackling air pollution that disproportionately impacts environmental justice communities, and organized a new public information campaign about potential health hazards associated with illegal idling of motor vehicles. That announcement included an online tip form, making it easier for residents to report incidents, and thus making it easier for the AG to investigate and/or bring similar actions going forward.

As another example, in December 2021, Healey, in connection with the U.S. Environmental Protection Agency and the Baker-Polito Administration, reached a settlement with Barnhardt Manufacturing Company, a cotton bleaching company, requiring the company to pay almost $1.5 million to settle allegations that it spilling dozens of gallons of acid in the North River, killing more than 270,000 fish and damaging more than 14 acres of protected wetland resource areas and over 12 acres of designated habitat of two state-listed rare species.

And while there have been a variety of other climate change and environmental enforcement actions across the years, there has arguably been no bigger case than Healey’s action against Exxon Mobil, which promises to remain active in 2022. In 2019, the AG’s Office filed suit against Exxon Mobil, alleging that the company engaged in a misinformation campaign about “the catastrophic climate impacts of burning fossil fuels.” Exxon Mobil sought dismissal on the grounds that its lobbying activity is free speech and falls within the broad definition of protected “petitioning” activity. It accuses Healey of bringing the suit for political reasons. In June 2021, a judge declined to dismiss the lawsuit, a decision that Exxon Mobil appealed. The Massachusetts Supreme Judicial Court is now set to hear oral argument in March, with Exxon Mobil pushing the same arguments the Superior Court dismissed. The case not only has big implications for the environmental space; should it go forward, it carries the potential to expand theories of liability that may ultimately be applied in other contexts.

Conviction Integrity

Healey is not solely concentrated on the AG Office’s past priorities; she is also expanding her focus in 2022. For example, on February 7, 2022, she announced the creation of a new Conviction Integrity Unit (CIU), further evincing that she plans to promote popular initiatives in her final year as AG. The press release describes the mandate of the CIU: “The CIU will re-investigate cases involving claims of innocence and claims that call into question the integrity of the office’s investigation and/or prosecution. Examples of potential conviction integrity concerns include police or prosecutorial misconduct, the unfairness of the process the defendant received, and newly discovered or available evidence that makes the conviction unreliable.” Look for more in this space in the coming year.
Review of Sanctions and Export Control Developments in 2021 and What to Expect in 2022

Posted on February 24th, 2022 by Shrutih Tewarie, Anthony Mirenda, Luciano Racco, Anna Annino, Daniel Zaleznik and Nick Bergara

This is the fifth post in this year’s series examining important trends in white collar law and investigations. Our previous post discussed trends in State AG enforcement. Up next: SEC Enforcement in 2022: A Look Ahead.

Key Takeaways:

- Russia and China will continue to be the focus of country-specific sanctions and export controls, but hotspots around the world persist;
- The Biden Administration will continue to focus on human rights, multi-lateral sanctions and export controls coordinated with allies, and the growing compliance threat posed by virtual currencies;
- Strong enforcement of sanctions and export control laws is expected to continue in 2022.

The first year of the Biden Administration featured a perhaps surprising degree of continuity with the Trump Administration’s international trade policies, although with an expected change in tone and emphasis on multilateral export controls and sanctions. We expect many of the same priorities from 2021 to continue in 2022, but with Russia overtaking China in the near term as the focus of U.S. concern.

A. Countries to Watch:

1. Russian Federation

Days before the end of the Trump Administration, the U.S. Department of the Treasury’s Office of Foreign Assets Control ("OFAC") imposed sanctions on a number of individuals and entities associated with election interference. The Biden Administration continued actively targeting Russia with new rounds of sanctions actions in response to a wide range of political disagreements and provocations. In March 2021, the Department of Commerce’s Bureau of Industry and Security ("BIS") announced expanded export restrictions pursuant to the determination that the Russian Government had used a prohibited weapon in the poisoning of opposition leader Alexei Navalny. BIS implemented new export restrictions prohibiting exports to certain military-intelligence end uses and end users ("MIEUs," and such restrictions, the "MIEU Rule"). The MIEU Rule places significant restrictions on exports to MIEUs in Russia and numerous other countries. In addition, the MIEU Rule prohibits U.S. persons from providing “support” to MIEUs, even if such support does not involve the export of items subject to the Export Administration Regulations ("EAR"). These actions were followed, in
April 2021, by the issuance of Executive Order 14024, which authorized sanctions on Russia in response to a range of “harmful foreign activities” by the Russian Government, including interference in U.S. elections, cyber-attacks against the U.S. and its allies, the use of transnational corruption to influence foreign governments, targeting of dissidents and journalists, and violation of international law. Under this new Executive Order, the OFAC quickly targeted a number of individuals and entities, including the SolarWinds cyber-attack, Russia’s continued military occupation of Crimea, and interference in U.S. elections. Controversially, in May 2021, the Biden Administration chose not to impose sanctions on Nord Stream 2 AG, a Russian-controlled company developing the Nord Stream 2 gas pipeline between Russia and Germany.

The final months of 2021 were dominated by Russia’s increasingly aggressive actions towards Ukraine. On February 21, 2022, following Russia’s recognition of the so-called Donetsk People’s Republic and Luhansk People’s Republic as independent from Ukraine, President Biden issued Executive Order 14065 imposing comprehensive sanctions on these regions, similar to the ones imposed on the Crimea region following its annexation by Russia. OFAC also issued several general licenses in tandem, including to allow a wind-down of operations and contracts involving the two regions by March 23, 2022, and to authorize the continued export of agricultural commodities, medicine and medical devices to the regions. The next day, on February 22, 2022, President Biden described Russia’s actions as “the beginning of a Russian invasion of Ukraine” and announced a second wave of sanctions, which OFAC swiftly implemented, along with issuing new FAQs and two general licenses to allow certain winding-down transactions. As a result of these actions, two Russian banks with ties to the defense industry (Corporation Bank for Development and Foreign Economic Affairs Vnesheconombank and Promsvyazbank Public Joint Stock Company) and their many subsidiaries, as well as several individuals associated with Putin’s “inner circle” and their family members were added to the SDN List. Additionally, OFAC published Directive 1A, which supersedes the prior Directive 1 and restricts U.S. participation in the secondary market for ruble or non-ruble denominated bonds issued by certain Russian financial institutions.

For a detailed analysis of potential sanctions and export controls that may be imposed in response to a further invasion of Ukraine by Russia, please see our client alert here. As this is a rapidly developing situation, Foley Hoag will be providing updates regarding any forthcoming Ukraine-related actions in future client alerts.

2. China

The Biden Administration has so far maintained a high degree of continuity with the Trump Administration’s approach to China, continuing to sanction China for undermining democracy in Hong Kong, imposing sanctions on Chinese military-industrial complex and Chinese surveillance technology companies, and taking action to promote human rights in China’s Xinjiang Uyghur Autonomous Region (“XUAR”).

The Trump Administration’s move to terminate preferential treatment of Hong Kong vis-à-vis the rest of China under the EAR and International Traffic in Arms Regulations (“ITAR”) was left in place by the Biden Administration. In January 2021, OFAC issued regulations to implement Executive Order 13936 of July 14, 2020, “The President’s Executive Order on Hong Kong Normalization,” which eliminated Hong Kong’s preferential treatment in a number of different areas, including sanctions, export controls, immigration, and academic exchanges. In March and December 2021, the State Department issued reports pursuant to the 2020 Hong Kong Autonomy Act, identifying several PRC and Hong Kong officials whose actions it deemed to have contributed to undermining Hong Kong’s autonomy. The identification of these individuals in the reports means that foreign financial institutions that knowingly conduct significant transactions with these individuals can now be subject to U.S. sanctions. In March 2021, China was included in the list of countries subject to BIS’s MIEU Rule. On July 16, 2021, OFAC also designated several PRC officials to the Specially Designated...
Nationals and Blocked Persons List (“SDN List”) pursuant to the Hong Kong Autonomy Act. On the same day, the U.S. Departments of State, Treasury, Commerce and Homeland Security also issued a business advisory to highlight growing risks that could adversely impact U.S. companies that operate in Hong Kong, including data privacy risks, risks regarding transparency and access to critical business information, and risks for businesses with exposure to sanctioned Hong Kong or PRC entities or individuals.

Further, in June 2021, President Biden issued Executive Order ("EO") 14032, “Addressing the Threat From Securities Investments That Finance Certain Companies of the People’s Republic of China,” which prohibits U.S. persons from purchasing or selling publicly-traded securities of any entities identified as Communist Chinese Military-Industrial Companies ("CMIC"), or any publicly traded securities that are derivative of such securities, or are designed to provide investment exposure to such securities. The new EO amends prior EO 13959 issued by President Trump, including by, amongst other things, expanding the scope of entities that may be subject to CMIC sanctions to include those operating in the surveillance technology sector of China. On February 15, 2022, OFAC issued regulations implementing EO 14032.

The Biden Administration also took various steps to punish and counter reported human rights abuses in China. In March and December 2021, OFAC sanctioned several PRC officials in connection with human rights abuses against ethnic minorities in XUAR. In December 2021, OFAC also added nine Chinese surveillance technology companies to the Non-SDN CMIC List for their role in developing and enabling technology that assist in tracking and identifying religious and ethnic minorities in XUAR. As explained below, U.S. Customs and Border Protection ("CBP") also issued various Withhold Release Orders ("WRO") targeting China and the XUAR in specific. The Biden Administration also passed the Uyghur Forced Labor Prevention Act on December 23, 2021, which essentially blocks the import of goods from the XUAR into the U.S.

These actions by the Biden Administration have generally been met with bipartisan approval. In light of the continued tension between China and the United States, we expect a steady rollout of sanctions and other trade restrictions targeting China to continue during the second year of the Biden Administration.

3. Afghanistan

2021 saw the return of Taliban control of Afghanistan after the withdrawal of U.S. coalition forces in August and the resulting swift collapse of the Afghan government. Although the Taliban has been designated as a Specially Designated Global Terrorist organization since 2001, in a much awaited FAQ released at the end of 2021, OFAC clarified that Afghanistan is not currently subject to comprehensive sanctions in the way that Iran, Syria, Cuba, North Korea, and the Crimea region of Ukraine are. As a result, sanctions on the Taliban and Haqqani Network (a semi-autonomous branch of the Taliban) generally do not prohibit U.S. persons from exporting or re-exporting goods or services to Afghanistan as long as the transactions do not involve persons on the SDN List. Further, in response to the uncertainty regarding how the Taliban designations impact interactions with the Afghan government, OFAC has issued multiple General Licenses (allowing certain humanitarian-related transactions), related FAQs, and a fact sheet, “Provision of Humanitarian Assistance to Afghanistan and Support for the Afghan People,” which provides an overview of the relevant exemptions and guidance.

We expect that the Afghan sanctions program will remain a priority for OFAC in 2022. Given that the Afghan government is now run by an organization designated on the SDN List, persons operating in Afghanistan are advised by OFAC to “use all information at their disposal when assessing their risk for sanctions exposure,” including by “supplementing internal due diligence information with an array of open-source material” to identify any potentially risky counterparties involved in a transaction.
4. Belarus

In response to what the U.S. deemed a fraudulent presidential election in Belarus on August 9, 2020, and the violent political repression that followed, the U.S. has launched five rounds of sanctions against the country in coordination with Canada, the EU, and the UK. Sanctions have targeted government officials and businesspeople as well as major petrochemical, potash (fertilizer), and tobacco product companies. Of particular note was the imposition of restrictions on dealings in new issuances of Belarusian sovereign debt in both the primary and secondary markets, which may serve as a model for future sanctions against Russia, which is currently subject only to restrictions on certain sovereign debt dealings in the primary market.

Although major industries in Belarus have already been heavily sanctioned, the risk of further sanctions against the country in 2022 remains very high, especially with the possibility that Belarus may assist Russia in a potential invasion of Ukraine.

5. Burma/Myanmar

Following the military coup d’état in Burma in early 2021, rather than re-activating the prior Burma sanctions regime, President Biden issued Executive Order 14014, “Blocking Property with Respect to the Situation in Burma,” authorizing sanctions on several categories of persons, including military personnel involved in the coup, as well as persons operating in the Burmese defense sector more broadly, or engaged in actions or policies that undermine democratic processes or institutions in Burma.

Since then, OFAC has designated various Burmese officials and entities to the SDN List pursuant to the EO, including most notably the State Administrative Council (“SAC”), which is the government body formed by the Burmese military to govern Burma. The most recent designations occurred on January 31, 2022, on the one-year anniversary of the military takeover in Burma, with OFAC adding to the SDN List seven individuals and two entities connected to Burma’s military regime. These designations were part of a joint action with the United Kingdom and Canada, who each also designated two Burmese government officials.

In March 2021, the Department of Commerce added Burma to the list of countries subject to Military End User controls as well as the MIEU Rule. In addition, on March 8, 2021, BIS downgraded Burma from Country Group B to Country Group D:1, which makes unavailable several license exceptions that previously could have been used to export certain items to Burma, and subjects the country to the more restrictive export licensing policy. The Departments of State, Commerce, Treasury, Labor, and Homeland Security and the Office of the U.S. Trade Representative also issued an advisory in January 2021 to inform entities and individuals of the heightened risks associated with doing business in the Burma, and in particular with the military regime.

We expect sanctions on Burma to continue in 2022, and for the U.S. to work alongside international allies to demonstrate the international community’s support for the people of Burma and to further promote accountability for the coup and the violence perpetrated by the regime.

6. Cambodia

The U.S. government has applied a number of sanctions in response to the suspicious activity, corrupt business schemes, and human rights violations that persist in Cambodia. In November 2021, the U.S. Commerce and Treasury Departments released a joint Cambodia Business Advisory on High-Risk Investment and Interactions where they publicized these issues and warned that companies engaging in business within
particular sectors of this country’s economy need to perform proper due diligence to avoid the legal challenges presented by various sanction regimes.

Later, in December 2021, BIS added Cambodia to Country Group D:5, leading to a restrictive review of Cambodian license applications concerning items controlled for national security reasons. This addition to the list also meant that Cambodia is now part of the group of countries that are subject to military end use/user (“MEU”) export controls. BIS also added Cambodia to the list of countries subject to the MIEU Rule and the State Department amended Section 126.1 of the ITAR to add Cambodia to the list of countries subject to an arms embargo.

7. Cuba

At the start of the year, expectations were that the Biden Administration would likely try to return to the thaw in U.S.-Cuba relations, as seen under the Obama Administration. However, in March 2021, Cuba was included in the list of countries subject to BIS’s MIEU Rule. Additionally, popular protests in Cuba in July 2021 resulted in the Biden Administration taking a tough line with the Cuban government, and there has been no material relaxation of sanctions on Cuba. We do not expect this to change in 2022—a federal election year.

8. Ethiopia/Eritrea

On September 17, 2021, President Biden issued Executive Order 14046, “Imposing Sanctions on Certain Persons With Respect to the Humanitarian and Human Rights Crisis in Ethiopia” in response to humanitarian conflict on the northern border of Ethiopia and Eritrea. The EO authorizes sanctions on persons who are found (directly or indirectly) to be responsible for, or complicit in activities that threaten the peace, security or stability of Ethiopia, and actions that obstruct the peace process in northern Ethiopia. All Eritrean military and security forces that operate in Ethiopia after November 1, 2020 are also subject to sanctions. Unlike many other OFAC sanctions regimes, the sanctions do not extend to entities which are owned 50% or more by an SDN designated pursuant to EO 14046. Following the issuance of the EO, OFAC issued general licenses for humanitarian purposes.

Several officials in the Eritrean government, along with the Eritrean military, have already been designated on the SDN List pursuant to EO 14046 for their destabilizing role in the conflict in Ethiopia. On February 9, 2022, OFAC also issued new Ethiopia Sanctions Regulations that implement the restrictions imposed in EO 14046. Additional guidance, FAQs, and general licenses will likely be forthcoming from OFAC in 2022 as OFAC intends to supplement the current regulations with more comprehensive regulations. We expect further sanctions on Eritrean officials and government agencies in 2022 if Eritrean military forces remain in Ethiopia.

In addition to the imposition of sanctions, on November 1, 2021, Ethiopia was added to Section 126.1 of ITAR, which subjects the country to an arms embargo. Eritrea was already listed in Section 126.1, which includes countries such as Afghanistan, Iraq, Libya, Russia, and Sudan, but its country policy was amended to remove a policy of granting licenses for certain non-lethal military equipment. Now, both Ethiopia and Eritrea are subject to a broad policy of denial for all export license applications under the ITAR.

9. Iran

On February 18, 2021, the Biden Administration rescinded the Trump Administration’s re-imposition of UN sanctions on Iran and formally offered to restart nuclear talks, which resumed later in the year. This raised the prospect of a thaw in relations with Iran. By all accounts, however, talks are not going well despite the Biden
Administration’s stated intent to rejoin the Joint Comprehensive Plan of Action ("JCPOA"). Instead, the Biden Administration imposed new sanctions on numerous Iranian persons throughout the year. In March 2021, Iran was also included in the list of countries subject to BIS’s MIEU Rule. We do not anticipate any material reduction in the scope of sanctions against Iran in 2022.

10. Nicaragua

In 2021, OFAC added multiple Nicaraguan government officials, government agencies, and state-owned entities to the SDN List for various human rights violations, including repression of civil society, supporting the fraudulent presidential and parliamentary elections, and undermining democracy and the rule of law.

In November 2021, OFAC added the Public Ministry of Nicaragua and nine Nicaraguan government officials to the SDN List following the fraudulent national elections held by the Ortega regime in that same month. Earlier this year, on January 10, 2022, OFAC added another six Nicaraguan government officials to the SDN List ahead of the inauguration of President Daniel Ortega and Vice President Rosario Murillo later that same day.

U.S. sanctions on Nicaragua have generally been met with international approval and support. Canada, the EU and UK have each also imposed sanctions on various entities and individuals in Nicaragua in the past year. We expect sanctions on Nicaragua to continue, and likely escalate, in 2022 in light of the Ortega regime’s continued human rights abuses and actions to undermine democratic processes.

11. Sudan

At the end of 2020, the Trump Administration removed Sudan from the list of state sponsors of terrorism, citing a return to democratic principles following a popular protest movement that led to the removal of long-time dictator, Omar al-Bashir, as well as the normalization of relations with Israel. Sudan was subsequently moved by BIS from Country Group E:1 to Country B, a much less restrictive designation from an export licensing standpoint, although it remains listed in Country Group D:5, which results in continued limitations on exports of arms to Sudan.

Sudan’s return to democracy was short-lived, as a military coup removed the civilian government in October 2021. The Prime Minister, Abdalla Hamdok, was restored to power in November after reaching a deal with Sudan’s military, but has since resigned again on January 2, 2022 in response to further violence by security forces against pro-democracy protesters. To date, there has been no move to impose sanctions on Sudan or to re-designate the country as a state sponsor of terrorism, but the situation is fluid and it is unclear who will lead the country in 2022, though the military will certainly remain a powerful force for the foreseeable future.

12. Venezuela

On January 19, 2021, the last day of the Trump Administration, OFAC designated three individuals, fourteen entities, and six vessels for sanctions evasion related to Venezuelan state-owned oil company Petroleos de Venezuela, S.A. ("PdVSA"). On March 11, 2021, the State Department issued additional blocking sanctions against President Nicolas Maduro pursuant to Executive Order 13949, “Blocking Property of Certain Persons with Respect to the Conventional Arms Activities of Iran” for assisting Iran with the acquisition of conventional arms and associated parts. As Maduro has been designated on the SDN List since 2017 pursuant to Executive Order 13692, this new action does not alter existing prohibitions but indicates that Venezuela’s economic ties with Iran remain an area of State Department focus. Also in March 2021, Venezuela was included in the list of countries subject to BIS’s MIEU Rule. During 2021, OFAC also extended several general licenses, including
extending the authorization for certain transactions with PdVSA, and issued a new general license on June 17, 2021 related to humanitarian assistance for the Covid-19 pandemic. While sanctions activity in 2021 was substantially lower than in preceding years, the Biden Administration has not significantly altered the Venezuela sanctions program, and continues to reject the regime of President Maduro, who has been in power since 2013. We expect to see the Venezuela sanctions program continue as long as the Maduro regime remains in power.

B. Other Areas to Watch:

1. International Criminal Court Sanctions

In June 2020, President Trump signed Executive Order 13928 authorizing the imposition of sanctions on foreign persons determined to have engaged in or assisted efforts by the International Criminal Court (“ICC”) to investigate or prosecute international crimes allegedly committed by Americans or personnel of certain United States allies, or to have materially assisted persons designated pursuant to EO 13928. On September 2, 2020, the Trump administration designated the ICC’s Chief Prosecutor, Fatou Bensouda, and the ICC’s Head of Jurisdiction, Complementarity, and Cooperation Division, Phakiso Mochochoko to the SDN List. On September 30, 2020, OFAC issued regulations to implement EO 13928.

The EO was the subject of a lawsuit filed by Foley Hoag in October 2020 in the U.S. District Court for the Southern District of New York on behalf of several plaintiffs, including Open Society Justice Initiative and four law professors, arguing that EO 13928 violates constitutional rights, including the plaintiffs’ freedom of speech. To read more about the lawsuit, see here and here.

The Biden Administration issued Executive Order 14022 on April 1, 2021, terminating the sanctions related to the ICC and OFAC issued a final rule removing the ICC Sanctions Program on July 6, 2021.

2. The Treasury 2021 Sanctions Review (the “Review”)

On October 18, 2021, the U.S. Department of the Treasury released a review of its economic sanctions programs administered by OFAC. The Review highlighted successes of the OFAC sanctions programs, including restricting Iran’s ability to fund its nuclear program and terrorist activities, and safeguarding tens of billions dollars’ worth of Libyan assets from misappropriation by former government officials. It also described considerations used by OFAC during the process of issuing sanctions, including whether a potential action: (1) has been sufficiently evaluated and approved as the most effective tool for the situation; (2) is part of a broader policy objective; (3) can cause potential unintended consequences on third parties; and (4) can be coordinated multilaterally with allies, stakeholders, or other interest groups.

However, the Review did not provide an examination of the impact of specific sanctions programs, or provide any new changes to existing OFAC guidance. Looking ahead, the Review indicates that we can expect to see a continued use of multilateral sanctions which, in addition to amplifying these sanctions programs’ political and economic impact, allows for greater information-sharing and collaboration, as well as a focus on tailoring sanctions programs to avoid interfering with humanitarian needs.

3. Virtual Currency

2021 saw a pronounced rise in scrutiny of virtual currencies by a range of U.S. regulators, including OFAC.
In November 2021, OFAC released its first ever guidance directed at members of the virtual currency industry regarding complying with OFAC sanctions requirements. Beyond putting the virtual currency industry on notice that OFAC is paying close attention to it, the guidance contained some specific best practices, including novel guidance on software tools that can enhance sanctions compliance. As in the past, OFAC recommended the use of geolocation tools, including Internet Protocol (“IP”) address blocking controls, for any platform dealing with virtual currency, as a safeguard to avoid contact with sanctioned jurisdictions. However, for what appears to be the first time, the guidance acknowledged that a simple geography-based IP screen may be insufficient, recommending that companies also monitor for known virtual private network (“VPN”) addresses to prevent users from masking their location. OFAC also recommended use of transaction monitoring and investigation software by making use of identifying information associated with virtual currency transactions. OFAC noted that it has been including certain known virtual currency addresses as identifying information for sanctioned persons on the SDN List. For more on OFAC’s guidance for the virtual currency industry, see our November 2021 client alert here.

The new guidance followed a number of other virtual currency-related enforcement actions by OFAC, including the designation of cryptocurrency exchange SUEX OTC, S.R.O. as an SDN on September 21, 2021 for facilitating financial transactions connected to ransomware operations. In addition, as covered below, OFAC also brought an enforcement action against BitPay, an Atlanta-based digital currency payment processor, for failing to conduct proper sanctions screens and due diligence on parties making digital currency payments on BitPay’s platform.

In light of the recent Senate testimony by Deputy Treasury Secretary Wally Adeyemo stating that the growth of digital currencies is one of the primary challenges to the continued effectiveness of U.S. sanctions regimes, we expect OFAC to continue to focus on the digital currency industry in 2022.

C. CFIUS Updates

The Committee on Foreign Investment in the United States (“CFIUS”) remains active and continues to focus primarily on transactions involving investors from China and Russia, though filings involving investors from China continued their precipitous decline from previous years. Although statistics for 2021 have not yet been released, on July 26, 2021, CFIUS released its annual report to Congress for calendar year 2020. The report showed that CFIUS assessed or reviewed 313 transaction-related filings (187 full notices and 126 short-form declarations), down slightly from 2019, when 325 filings were reviewed. CFIUS entered into mitigation agreements in connection with 16 notices filed in 2020. Of the 313 filings, only 22 (17 notices and 5 declarations) involved China. CFIUS notices related to China are down nearly 75% from 2018 levels. Although some of the decline is likely pandemic-related, it is also clear that Chinese investors are increasingly avoiding transactions that require, or could invite, CFIUS scrutiny.

The most significant CFIUS enforcement action of 2021 involved a SPAC transaction between Stable Road Acquisition Corp. and Momentus Inc., a U.S. commercial space company offering transportation and other in-space infrastructure services, whose co-founders were Russian. In order to address CFIUS’s concerns, on June 9, 2021, Momentus entered into a National Security Agreement (“NSA”) with the Department of Defense and Department of the Treasury as lead agencies on behalf of CFIUS. As part of the NSA, Momentus’s Russian co-founders divested from the company, and Momentus engaged a third-party monitor, hired key positions to provide additional oversight, and appointed a CFIUS-approved director to its board to oversee compliance with the NSA’s stipulations.
For 2022, we expect CFIUS to continue to focus on transactions involving Chinese and Russian investors (including those that are not notified to CFIUS), as geopolitical tensions with both countries continue to rise. In addition, Congress is considering the U.S. Innovation and Competition Act (“USICA”), which includes the Strategic Competition Act that, if enacted, will expand CFIUS’s jurisdiction to include certain foreign gifts and contracts to institutions of higher education that equal or exceed $1 million in a single year, or aggregate gifts or contracts from the same foreign source valued over $1 million during a two-year period. USICA has bipartisan support and passed the Senate in June 2021, and is now with the House of Representatives. President Biden urged its passage as recently as January 21, 2022.

D. Withhold Release Orders

Through the issuance of WROs, CBP continues to use its enhanced authority under the Trade Facilitation Act of 2015 to block the import of goods made in whole or in part with forced labor.

In fiscal year 2021, there were seven WROs and two findings issued, as well as 1,469 shipments detained. There was also movement regarding modifying or revoking existing WROs. Four WROs and one finding of forced labor were modified or revoked in 2021, which indicates that CBP is working closely with importers and evaluating new evidence during their investigation process.

The WROs issued in 2021 focused primarily on China—in particular, the Xinjiang region, where Uyghurs and other minority groups have been subject to forced labor and other human rights violations—as well as on palm oil and rubber gloves from Malaysia and seafood from deep sea fishing vessels. With the signing of the Uyghur Forced Labor Prevention Act (the “Act”) on December 23, 2021, there now is a rebuttable presumption that all goods from Xinjiang are made with forced labor and, as a result, will be blocked from import into the U.S. unless the importer can present evidence overcoming this presumption. CBP will be providing guidance regarding what due diligence is necessary to determine that products do not originate from Xinjiang. The Act will take effect on June 21, 2022, so we expect to see a flurry of activity in the upcoming months related to imports from China.

The palm oil and fishing industries will likely remain a focus for CBP, but we also expect to see attention on other high-risk areas, such as cacao farming and the extractive industries. Five WROs and two findings have already been issued in fiscal year 2022, which shows that forced labor enforcement actions will remain a highly active area in the upcoming year.

E. Enforcement Trends

In 2021, OFAC brought enforcement actions against 19 different companies and one individual. These actions highlight several different enforcement trends that we expect will continue in 2022.

1. Non-U.S. companies continue to face enforcement risk for non-compliance with OFAC sanctions.

OFAC has brought enforcement actions against several different non-U.S. companies over the past year, highlighting the broad reach of OFAC’s sanctions programs and the importance of OFAC sanctions compliance for non-U.S. companies engaged in international trade and commerce.

In January 2021, OFAC entered into a $1,016,000 settlement with PT Bukit Muria Jaya (“BMJ”), an Indonesian paper products manufacturer, for violations of the North Korea sanctions program arising from BMJ’s exportation of cigarette paper to intermediary entities located in, or doing business on behalf of, North
Korean entities. BMJ directed payments for its DPRK-related exports to its U.S. dollar bank account at a non-U.S. bank, which in turn caused wire transfers related to such exports to clear through U.S. banks. Even though the payments originated from, and were directed to, a non-U.S. bank, OFAC found that these transactions violated U.S. sanctions because they caused U.S. financial institutions to engage in the prohibited exportation of services to North Korea, a comprehensively sanctioned jurisdiction.

Similarly, in March 2021, OFAC entered into a $950,000 settlement with Italian company Nordgas s.r.l. (“Nordgas”) for apparent violations of the Iranian Transactions and Sanctions Regulations (“ITSR”) that occurred when Nordgas reexported shipments of air pressure switches procured from a U.S. company to customers in Iran. OFAC found that Nordgas had taken several steps to conceal from the U.S. supplier that the shipments were intended for customers in Iran, causing the U.S. company to indirectly export its goods to Iran in violation of U.S. sanctions.

More recently, at the beginning of this year on January 11, 2022, OFAC entered into a $5,228,298 settlement with Sojitz (Hong Kong) Limited (“Sojitz HK”), a Hong Kong, China-based offshore trading and cross-border trade financing company for apparent violations of the ITSR. The violations occurred when Sojitz HK made U.S. dollar payments from its Hong Kong bank to purchase Iranian-origin high density polyethylene resin from a supplier in Thailand for resale to buyers in China. These U.S. dollar payments were processed and settled through multiple U.S. financial institutions, including the U.S. correspondent banks of Sojitz HK’s Hong Kong bank and the supplier’s Thai banks, resulting in violations of OFAC’s Iran sanctions program.

As these enforcement actions show, non-U.S. companies should remain vigilant regarding the U.S. sanctions prohibitions that could apply to their activities, particularly where those activities involve U.S. persons, U.S.-origin goods, or the U.S. financial system. Even where a non-U.S. company does not itself engage in a violation of U.S. sanctions, it may nonetheless face liability for U.S. sanctions violations when it causes a U.S. person to engage in a prohibited transaction.

2. Companies may be liable for sanctions violations engaged in by their business partners or customers.

Continuing a trend from prior years, in 2021, OFAC brought several enforcement actions against companies for violations engaged in by their business partners or customers, highlighting the importance for companies to engage in proper diligence on parties with whom they transact.

For example, in April 2021, OFAC announced a settlement with SAP SE (“SAP”), a software company headquartered in Germany, to resolve an investigation into apparent violations by SAP of the Iran sanctions program. The violations occurred when third-party resellers of SAP’s software licenses and related maintenance services sold those licenses and services to entities that provided the SAP software to users in Iran. OFAC faulted SAP for, amongst other things, failing to conduct proper due diligence on its third-party resellers, especially given that some of them publicized their business ties with Iranian companies on their websites. A more detailed overview of SAP’s settlement with OFAC, along with concurrent settlements entered into between SAP and the U.S. Department of Justice and BIS can be found here.

Similarly, in March 2021, OFAC entered into a settlement with UniControl, Inc. (“UniControl”), a Cleveland, Ohio-based entity that manufactures process controls, airflow pressure switches, boiler controls, and other instrumentation, for exporting multiple shipments of its goods to two European companies that then reexported the goods to Iran in violation of the ITSR. OFAC found that UniControl had ignored several red flags based on which it had reason to know that the goods would be reexported to Iran by its European trade partners. Those red flags included obfuscated end-user requests, an expressed interest in supplying
UniControl’s goods to Iranian customers, and requests to remove “Made in USA” labels from UniControl’s products, by UniControl’s European trade partners.

3. Continued focus on digital currency companies.

In April 2021, OFAC announced the settlement of its enforcement action against BitPay, an Atlanta-based digital currency payment processor, for violations of various sanctions programs. BitPay conducted due diligence on its direct customers – i.e. the merchants on its platform – including by screening them against OFAC’s SDN List; however, BitPay failed to screen the merchant’s buyers, even though BitPay had access to the buyers’ names, addresses, email addresses, and phone numbers, and eventually also obtained access to their IP addresses. As a result of BitPay’s compliance failures, buyers in Crimea, North Korea, Iran, Sudan, and Syria were able to enter into digital currency transactions with U.S. merchants on BitPay’s platform.

This is OFAC’s second enforcement action involving a company in the digital currency space (the first enforcement action was brought at the end of 2020 against BitGo, Inc., a technology company that provides digital asset custody, trading, and finance services). As set forth above, we expect that digital currency companies will continue to face increased scrutiny by OFAC going forward.

The Department of Justice’s National Security Division (“NSD”) was also very active in 2021, bringing 50 cases with the majority involving violations of Iranian sanctions or unauthorized transactions with Chinese persons (including violations of export control laws). NSD also reported an uptick in voluntary disclosures to the division and highlighted the benefits of disclosing willful conduct including the reduced penalties given to SAP. We expect NSD will continue to focus on unauthorized activity involving Iran, China, Russia, and North Korea in 2022. In addition, we expect there to be a focus on human rights violations and the use of cryptocurrency transactions as a means to evade sanctions and engage in money laundering.

The State Department’s Directorate of Defense Trade Controls (“DDTC”) entered into two consent agreements in 2021 with companies who violated the ITAR. In April 2021, DDTC announced a consent agreement with Honeywell International, Inc. (“Honeywell”) for alleged violations of the Arms Export Control Act and the ITAR including unauthorized exports and retransfers of ITAR-controlled technical data to China. DDTC found that the exports of technical data to China threatened U.S. national security by including drawings for certain parts and components of the F-35, F-22, and B1-B aircraft platforms and the CTS800 engine platform. The consent agreement requires Honeywell to engage an external “Special Compliance Officer” to oversee the consent agreement for at least 18 months and imposed a civil penalty of $13 million with $5 million suspended if the money is used toward DDTC-approved corrective actions to strengthen Honeywell’s compliance program. Aggravating factors included the recurrence of violations previously disclosed in 2016, harm to national security, and the involvement of an ITAR Section 126.1 country (China) and Significant Military Equipment.

In August 2021, DDTC announced a consent agreement with Keysight Technologies, Inc. (“Keysight”). In November 2017, DDTC expressed concerns to Keysight that its Multi-Emitter Scenario Generation software may be subject to the ITAR and recommended the submission of a commodity jurisdiction request (“CJ”) to resolve those concerns. Keysight had self-determined that software as subject to the EAR and controlled it as EAR99. In January 2018, Keysight submitted the CJ, but continued to export the software as EAR99 (including to China) while the commodity jurisdiction was pending. In April 2018, DDTC responded to the CJ by determining that the software is subject to the ITAR. The consent agreement, the result of unauthorized exports to China during the pendency of the CJ request, requires Keysight to engage an external Special Compliance Officer to oversee the consent agreement and imposed a civil penalty of $6.6 million with $2.5
million suspended if the money is used toward DDTC-approved corrective actions to strengthen Keysight’s compliance program.

The Department of Commerce’s Office of Export Enforcement announced 19 public settlements in 2021 focusing on cases involving concealment of violations (i.e. failing to voluntarily disclose violations), non-US companies who use U.S. persons to conduct illegal exports, and cases involving emerging technologies and the use of virtual currencies.

Overall, strong enforcement of sanctions and export control laws is expected to continue in 2022.

---

**SEC Enforcement in 2022: A Look Ahead**

Posted on February 28th, 2022 by John Murray and Christian Garcia

*This is the sixth post in this year’s series examining important trends in white collar law and investigations. Our previous post discussed trends in sanctions & export controls enforcement. Up next: trends in False Claims Act enforcement.*

**Takeaways:**

- The SEC Division of Enforcement’s increasingly aggressive pursuit of investigations and enforcement actions will continue in 2022.
- Stiffer corporate penalties and a more restrictive approach to cooperation credit are likely over the coming year.
- Enforcement will continue to focus on longstanding priorities such as insider trading and private fund disclosures, while intensifying its scrutiny in newer areas including ESG, cyber enforcement, and SPACs.
- The SEC’s highly successful whistleblower program will continue to feed the Enforcement pipeline and encourage employees to report wrongdoing to the agency.

During 2021, the U.S. Securities and Exchange Commission (“SEC”) met expectations that the agency’s enforcement program would move in a more aggressive direction under the Biden administration. Through the rhetoric of its leadership and its enforcement actions, the SEC has signaled a tougher stance on areas of longstanding interest such as insider trading and investment adviser disclosure, as well as more recent priorities such as ESG investing and cryptocurrency. (We discussed the outlook for enforcement of the Foreign Corrupt Practices Act, another long-established SEC priority, in a prior post.) In particular, this shift was reflected in numerous public statements by SEC Chairman Gary Gensler, who formerly served as the generally pro-enforcement Chairman of the U.S. Commodity Futures Trading Commission, and by the Director of the SEC’s Division of Enforcement (“Enforcement”) Gurbir Grewal, who
joined the SEC last year after serving as New Jersey’s Attorney General, and before that, Chief of the Economic Crimes Unit in the U.S. Attorney’s Office for the District of New Jersey.

Enforcement activity since Gensler’s arrival has followed suit. Despite the operational difficulties that the COVID-19 pandemic has posed for Enforcement, the SEC in fiscal year 2021 brought 434 “stand-alone” actions (enforcement actions excluding those brought against issuers for delinquent filings and “follow-on” administrative proceedings seeking bars against individuals), representing a 7 percent increase over fiscal year 2020. Enforcement likewise collected $1.4 billion in penalties, a 33 percent increase from fiscal year 2020. However, the total disgorgement amount obtained by the Division – $2.4 billion – was down by 33 percent. We believe that this decline is an anomaly and will be reversed in 2022, given Enforcement’s tougher posture and the expanded disgorgement power that Congress gave the agency in last year’s National Defense Authorization Act (“NDAA”). (See here for our prior discussion of the Act and its implications for Enforcement.)

We expect Enforcement this year to continue executing the priorities articulated by Gensler and Grewal, which we discuss in detail below.

**Significant Procedural Changes**

In order to streamline and expedite its investigations, the SEC last year reversed some significant procedural changes that it had adopted during the Trump administration. Last February, then Acting Chair Allison Herren Lee announced that the SEC would be restoring its previous policy of allowing senior officers to approve Formal Orders of Investigation, which empower Enforcement staff to issue subpoenas and take sworn testimony. The Commission under former Chairman Jay Clayton ended that policy in 2019, requiring the staff to obtain approval from the Commission or the Director of Enforcement, a move that some criticized as hampering the staff’s ability to move investigations along efficiently. The restoration of decentralized Formal Order authority frees the Division from the “red tape” required by the prior practice and will allow Enforcement staff to move more quickly in gathering evidence.

The SEC also reversed a policy implemented in 2019 that permitted parties to submit settlement offers conditioned upon waivers by the Commission of the automatic statutory disqualifications that result from certain violations of the securities laws, such as the loss of well-known seasoned issuer (“WKSI”) status or ineligibility to conduct private offerings under Regulation D. The reversal restores the SEC’s previous policy requiring parties to separately submit offers of settlement to Enforcement and requests for waivers to the Division of Corporation Finance or the Division of Investment Management. The change also suggests a more skeptical view of waiver requests, with the result that settling parties may have a harder time convincing the staff that a waiver is appropriate. It will also result in greater uncertainty for settling parties, who face the prospect of agreeing to offers of settlement without any assurance of a waiver.

**Return of Settling Party Admissions**

In October, Grewal announced that Enforcement planned to restore the Obama-era policy of requiring admissions by settling parties in cases involving serious or egregious misconduct. The SEC has historically permitted defendants to settle enforcement actions on a “neither admit nor deny” basis, whereby the defendant agrees to specific sanctions and penalties without admitting or denying the SEC’s allegations. The SEC adopted a similar policy in 2013 under former Chair Mary Jo White, but in practice, rarely required admissions, and Enforcement under her successor, Jay Clayton, distanced itself from the approach.
It remains to be seen whether Enforcement will seek admissions more frequently than was the case under White. If so, this change could have significant consequences for settling entities that face the prospect of private litigation, in which their admissions could be binding. The possibility may lead more companies to litigate the SEC’s charges rather than accept settlements that would require them to admit wrongdoing.

**Harsher Sanctions Forthcoming**

The SEC’s leadership has also indicated an intent to make broader use of the remedies and relief in its arsenal. For one, Grewal reported last year that Enforcement will consider seeking officer and director bars, which prevent individuals from serving as executives or directors of public companies, not only against individuals currently serving in public companies, but also against those who no longer serve in public company roles but might do so again in the future.

Harsher corporate penalties are likewise on the agency’s agenda. Democratic commissioners (who are currently in the majority) have historically tended to be more supportive of corporate penalties than their Republican counterparts. Moreover, Grewal has warned that the SEC will pursue higher penalties against companies who violate “a law or rule for which the SEC has previously and publicly charged other actors in their industry[.]” It remains unclear how this guideline will operate in practice. Taken literally, it could be understood to include any company charged with a first-time violation that the agency has long pursued, such as misleading disclosure or inadequate internal controls. Whether the securities laws authorize the SEC to obtain higher penalties under such circumstances, however, is subject to question, and we expect that this approach would invite challenge in the courts if the SEC were to apply it in such a broad manner.

Following the lead of the U.S. Department of Justice (“DOJ”), with which Enforcement frequently works in parallel, the SEC has also communicated a more rigid stance on cooperation credit. Last October, Deputy Attorney General Lisa Monaco announced that the DOJ would be restoring previous guidance requiring cooperators to provide the government with “all non-privileged information about individuals involved in or responsible for the misconduct at issue.” This is a stricter standard than the previous DOJ policy, which allowed credit where cooperators identified individuals “substantially involved in the misconduct.” One week after Monaco’s remarks, Gensler clarified that the DOJ’s new policy was “broadly consistent with [his] view of how to handle corporate offenders.” Parties seeking credit under this heightened standard will thus face a heavier burden, and may encounter greater pushback from Enforcement with respect to the adequacy of their disclosures, in negotiating deferred prosecution and non-prosecution agreements with both the SEC and DOJ.

**ESG at the Forefront**

The SEC has in recent years become increasingly attentive to – and concerned about – the rising prominence of environmental, social, and governance (“ESG”) investing. In particular, Enforcement has been scrutinizing statements by investment advisers and issuers characterizing their investment practices as ESG-compliant.

The agency last year continued to make significant investments in its ESG expertise and capabilities. In February, it announced the appointment of a Senior Policy Advisor for Climate and ESG. In March, Enforcement created a Climate and ESG Task Force, with the mission of “develop[ing] initiatives to proactively identify ESG-related misconduct” and using the SEC’s analytical capabilities to “mine and assess information across registrants” to identify potential securities violations. The Task Force is also charged with the initial task of “identify[ing] any material gaps or misstatements in issuers’ disclosure of climate risks under existing rules,” and will similarly focus on ESG-related disclosures by advisers. Last April, the Division of Examinations, with which Enforcement routinely collaborates in building its investigations, issued a Risk Alert targeted at
advisers, identifying “potentially misleading statements regarding ESG investment processes” and “representations regarding the adherence to global ESG frameworks.”

Together, these developments portend a continued ratcheting up of ESG-focused enforcement activity. In particular, the allocation of resources to the Task Force is a strong indicator of Enforcement’s belief that issuers and advisers have been falling short in complying with their disclosure obligations and that enforcement action is needed.

_Private Funds in the Crosshairs_

Enforcement attention on private funds is not new, and the SEC has indicated that they will remain a central focus under Gensler. The Chairman last year repeatedly expressed his view that the growth of private funds, coupled with what he sees as their lack of transparency, invite more exacting regulation. In May, he noted in testimony before the House Subcommittee on Financial Services that there has been a 58 percent increase in private equity funds over the prior five years, and emphasized the importance of holding advisers to those funds accountable for violations of the securities laws. He also observed that Enforcement is focused in particular on disclosure of investment risks, conflicts of interest, and controls around the dissemination of material non-public information (“MNPI”). Gensler expressed similar sentiments before the Senate Committee on Banking, Housing, and Urban Affairs in September.

In addition, the Division of Examinations last June issued a Risk Alert with respect to advisers to private funds, finding widespread deficiencies in advisers’ disclosure of conflicts, allocation of fees and expenses, and policies and procedures with respect to MNPI. In January of this year, it issued another Risk Alert focused on private fund advisers, noting conduct inconsistent with disclosures to investors (for example, failure to obtain informed consent from Limited Partner Advisory Committees and failure to comply with Limited Partnership Agreement liquidation terms), misleading disclosures concerning performance and marketing, due diligence failures, and potentially misleading use of hedge clauses. Given that the Division of Examinations regularly refers its findings to Enforcement, the Risk Alert provides a further signal that 2022 will continue to see enforcement actions arising in these areas.

_Continuing Crackdown on the Cryptocurrency and Cybersecurity Front_

Cryptocurrency and cybersecurity have been priorities for Enforcement dating at least back to the formation of Enforcement’s Cyber Unit in 2017. The Division’s focus on these areas has intensified under Gensler, who last August, likened the crypto space to the “Wild West,” and cautioned that the crypto asset class is “rife with fraud, scams, and abuse.” Accordingly, he has instructed SEC staff to vigorously pursue unregistered sales of digital assets under the Securities Act of 1933 and related misconduct. Enforcement has been busily carrying out this directive, last year charging promoters of an allegedly fraudulent $2 billion digital asset securities offering; bringing its first enforcement action involving securities using a decentralized finance platform, or “DeFi,” technology; pursuing an operator of an allegedly unregistered online digital asset exchange; and halting registration of two digital tokens due to an allegedly fraudulent SEC Form 10. The trend has continued into 2022. The SEC last month obtained a $100 million penalty — the largest in a crypto enforcement action — against a provider of crypto lending accounts for allegedly failing to register its product under the Securities Act or itself as an investment company under the Investment Company Act of 1940, and for misrepresenting the level of risk in its lending business.

Cybersecurity, including the failure of issuers to fully disclose data breaches and of investment advisers to maintain required cybersecurity protocols, remained an Enforcement priority in 2021. There were multiple
high profile disclosure cases, including an enforcement action charging a company with failing to maintain adequate disclosure controls based on allegations that executives were not apprised of a potential vulnerability with respect to customer data or the company’s failure to take steps to address it, and an enforcement action claiming that a public company delayed disclosing and downplayed a 2018 data breach involving customer accounts and student records.

Enforcement also continued to bring enforcement actions for violations of Regulation S-P, otherwise known as the “Safeguards Rule,” which requires registered broker-dealers, investment companies, and investment advisers to adopt written policies and procedures establishing safeguards for the protection of customer records. Last month, the SEC announced proposed new cybersecurity risk management rules for registered investment advisers, registered investment companies, and business development companies, which, if adopted, will broaden the range of charges available against those entities for cybersecurity and related disclosure failures. We therefore anticipate that Enforcement’s close scrutiny of cybersecurity practices and disclosures will continue over the coming year.

**Insider Trading Regaining Prominence**

Historically an SEC priority, insider trading enforcement fell markedly under the Trump administration. We expect that trend to reverse in 2022. Grewal set the tone for more aggressive insider trading enforcement in an October 2021 speech premised on Enforcement’s “responsibility to maintain market integrity and enhance public trust in our securities markets.”

Even before Grewal’s remarks, the SEC had begun to push the boundaries of insider trading law in its first enforcement action based on so-called “shadow trading,” a novel theory under which an individual may be liable for trading in the securities of a company to which he or she has no relationship, but whose securities are somehow correlated to those of a company to which he or she owes a duty. In that case, the SEC alleges that a former executive of a mid-sized, oncology-focused biopharmaceutical company purchased short-term, out-of-the-money stock options in another mid-cap oncology-focused biopharmaceutical company shortly before the public announcement that his company would be acquired at a significant premium, and after learning that the other company’s share price was likely to increase following the announcement. While the action survived a motion to dismiss in January, further shadow trading cases are very likely to be litigated, and it remains to be seen whether other courts will validate the theory.

The use of “10b5-1 plans,” which provide an affirmative defense to corporate insiders who make predetermined securities trades, subject to certain conditions set forth in SEC Rule 10b5-1, is also likely to attract heightened Enforcement attention over the coming year. Critics have long contended that 10b5-1 plans can be gamed – allowing insiders to trade on MNPI – by revising or cancelling them, or crafting them to allow trading shortly after adoption of a plan. Gensler has expressed agreement with these views, noting last June that the plans currently “lead to real cracks in our insider trading regime,” and requested recommendations from the staff for proposed revisions to Rule 10b5-1. The SEC accordingly proposed a series of amendments to the Rule in December, which, among other things, would narrow the circumstances under which plans may be adopted and require written certifications from directors and officers that they are not aware of MNPI at the time of adoption. Thus, the new requirements would narrow the circumstances in which a 10b5-1 plan will preclude the SEC from bringing insider trading charges.

**SPACs Under Intensifying Scrutiny**

U.S. securities markets in 2020 and 2021 saw a surge in the use of special purpose acquisition companies, or
SPACs, as an alternative method for taking a private company public. A SPAC is a shell company with no operations created for the sole purpose of raising capital through its own IPO so that it can acquire or merge with a privately held company. Gensler last year repeatedly expressed concern about insufficient disclosure of the conflicts of interest inherent in, and the dilutive effects of, SPACs, among other aspects of these deals. He has called for recommendations to address these risks, and publicly called upon Enforcement to continue its focus on SPACs.

Last July, the SEC brought its first enforcement action against a SPAC, charging the target of a SPAC transaction with misrepresenting the success of its technology and the likelihood that it would secure necessary governmental approvals, and the SPAC itself with repeating those misstatements to investors while overstating the due diligence it had conducted on the target. While the frequency of SPAC transactions has fallen significantly since last year, the proliferation of these deals in recent years, along with Gensler’s instruction that Enforcement prioritize SPAC investigations, suggest that more SPAC-related enforcement actions are likely in 2022.

**Whistleblower Program Will Continue to Drive Enforcement**

The SEC’s Whistleblower Program has continued its dramatic expansion in recent years, providing powerful incentives to employees and other whistleblowers with headline-making awards. The Program had a record-breaking year in fiscal 2021, during which the SEC awarded approximately $564 million to 108 different individuals, representing the largest dollar amount and the largest number of award recipients in a single fiscal year. Last year also saw the two largest awards in the program’s history, including a $110 million award in September and a $114 million award in October. To date, the Program has awarded over $1 billion since its inception in 2012. We expect that Enforcement will continue to enthusiastically leverage the Program as a source of enforcement actions yielding large disgorgement and penalty amounts.

In addition to ratcheting up the size of whistleblower awards, the SEC is poised to reverse controversial changes to the Whistleblower Program rules made under the Trump administration. In 2020, Republican commissioners approved amendments and interpretive guidance which, among other changes, (1) made actions brought by another agency or regulator ineligible for SEC whistleblower awards in cases where the Commission determined that the other agency or regulator had a whistleblower program that “more appropriately” applied to the action, and (2) effectively gave the SEC discretion to reduce the amount of the largest awards based on their dollar amounts. These changes drew vigorous criticism from Democratic commissioners and the plaintiffs’ bar. Last month, the SEC announced two proposed amendments that would largely undo the Trump-era changes by expressly authorizing awards where the other whistleblower program would result in a significantly lower award than the SEC would pay, and by limiting the Commission’s discretion to consider the dollar amount of an award only to increase, not reduce, an award. The proposed amendments underscore the Gensler Commission’s aim of incentivizing whistleblowers to report wrongdoing as well as the continuing importance for companies to have effective internal processes for reporting and investigating potential misconduct.

We will continue to follow and provide updates on Enforcement activity and priorities throughout the year.
False Claims Act Enforcement in 2022: What To Expect In The Year Ahead

Posted on March 3rd, 2022 by Neil Austin and Natalie Panariello

This is the seventh post in this year’s series examining important trends in white collar law and investigations. Our previous post discussed SEC Enforcement in 2022: A Look Ahead. Up next: ESG and the SEC: What’s Next on the Horizon.

Looking further ahead into 2023, we expect to see several trends in the DOJ’s enforcement of the False Claims Act:

- First, continuing a trend that began in the Trump administration, we expect the total number of cases brought under the False Claims Act to continue to climb, fueled in part by a continued focus on bringing cases directly rather than relying on whistleblowers—often as a result of the government’s increasing reliance on data analytics.
- Second, we expect the health care industry to continue to receive the lion’s share of enforcement scrutiny, with particular focus on telehealth services, Medicare Advantage fraud, medically unnecessary procedures, and alleged kickbacks.
- Third, we expect an increasing use of the False Claims Act to ensure compliance with cybersecurity standards and to stamp out alleged pandemic fraud.

Steady Flow Of New Matters Fueled By Data Analytics

As discussed in last year’s post, the period between 2017 and 2020 was the most active period of enforcement in the False Claims Act’s history as measured by the number of new matters opened. That increased activity was the result of sharp increases in the number of cases brought directly by the government rather than through qui tam relators, or whistleblowers. In contrast to the period 2013-2016, when the government brought an average of 118 cases per year, the government brought an average of 170 cases per year between 2017 and 2020, with a high of 259 cases in 2020. The first year of the Biden administration showed a continuation of that trend, with 203 government-brought cases—more than 25% of the total number of new matters brought in 2021.

In remarks delivered last year at the Federal Bar Association Qui Tam Conference, Principal Deputy Assistant Attorney General for the Civil Division, Brian Boynton, alluded to continued efforts by the DOJ to expand its role in identifying and bringing cases directly, including through the use of data analytics. According to Boynton, “our sophisticated data analytics allows us to identify patterns across different types of health care providers – giving us a way to identify trends and extreme outliers.” In addition to allowing the government to “see where the highest risk physicians are located in each state and federal district,” the data analytics also allows the government to “demonstrate and quantify sophisticated relationships, such as a physician offering controlled substance prescriptions to a patient who is likely to divert them” and, additionally, to target COVID-19 related misconduct.
Looking ahead, we expect the FCA enforcement landscape to be shaped by increasing numbers of cases brought by the government directly, and we expect this trend to continue as the government devotes more resources to the analysis of massive amounts of billing data at its fingertips.

**Health Care**

Health care has been and almost certainly will remain the largest sector targeted by DOJ for FCA enforcement. Indeed, of the more than $5.6 billion in settlements and judgments reported by the DOJ in financial year 2021, over $5 billion related to cases involving the health care industry. We expect this trend to continue this year.

In particular, we expect continued focus in the area of telehealth. As a result of the COVID-19 pandemic and pandemic-related policies intended to improve access to care, telehealth services have expanded. This expansion has resulted in alleged abuses, and DOJ has targeted those abuses both criminally and civilly. For example, last May, the Department announced first-in-the-nation charges relating to the exploitation of the expanded telehealth policies arising from the submission of false and fraudulent claims for telemedicine encounters that allegedly did not occur.

Relatedly, we expect to see continued enforcement surrounding unnecessary medical services and services not rendered as billed. The Department has signaled a focus on schemes that target elderly patients by providing them poor or unnecessary care or no care at all. For example, in 2021, the Department reached an eight-figure settlement with a nursing home operator for alleged false claims relating to unreasonable and unnecessary rehabilitation therapy services and substandard skilled nursing services.

The Medicare Advantage Program, also known as Medicare Part C, has also been an important priority for the DOJ. Medicare Part C pays a capitated amount to private health insurance carriers for each patient enrolled in their plans. Those payments are adjusted for various risk factors such that plans receive higher payments for higher-risk enrollees. The DOJ has zeroed in on plans and providers that manipulate this risk adjustment process to increase payment amounts. For example, in August of last year, DOJ announced a $90 million FCA settlement with a California-based health care services provider to resolve allegations that it submitted inaccurate information about the health status of beneficiaries enrolled in Medicare Advantage Plans. We expect enforcement actions of this sort to continue this year.

Finally, we expect continued FCA enforcement targeting kickbacks. In 2021, the Department resolved matters relating to kickback violations involving companies across the health care industry, including an electronic health record vendor, home health care agencies, hospitals, substance abuse treatment facilities, pharmaceutical companies, diagnostic testing companies, and medical device companies. Given this breadth, companies across the health care sector should direct their attention towards compliance with the Anti-Kickback Statute.

**Cybersecurity**

Our prediction last spring that the DOJ would focus FCA enforcement efforts in the area of cybersecurity proved prescient. As we reported in October, the Department announced the launch of a new Civil Cyber-Fraud Initiative that will use the FCA to prosecute cyber vulnerabilities and incidents that arise with government contracts and grants. According to Deputy Attorney General Lisa Monaco, the Department aims to “drive cybersecurity accountability” through FCA enforcement. And while the Department “take[s] very
seriously [its] mission to help victims of cyber intrusions,” victims who fail, for example, to timely report suspected breached may be punished with civil fines.

Indeed, in a speech at the Cybersecurity and Infrastructure Security Agency (CISA) Fourth Annual National Cybersecurity Summit, Mr. Boynton described three “common cybersecurity failures” that the Department views as “prime candidates” for potential FCA enforcement: (1) knowing failures to comply with cybersecurity standards; (2) knowing misrepresentations of security controls and practices; and (3) knowing failures to timely report suspected breaches. Importantly, the initiative will focus on cases affecting federal agencies and sensitive government information and systems. Entities that provide the government with cyber products and services should therefore take warning of DOJ’s new focus in this area, as FCA growth in this area is likely in the coming years.

**Pandemic Fraud**

Finally, we expect to see a continued emphasis on using the False Claim Act to curtail pandemic-related fraud. With the Attorney General having established a COVID-19 Fraud Enforcement Task Force in May of 2021, expect to see a steady stream of pandemic-related matters over the coming year. The AG’s announcement of the Task Force highlighted the variety of alleged frauds arising out of the pandemic and foreshadowed the areas of likely activity:

*The pandemic has given rise to a variety of forms of fraud. Those intent on unlawfully profiting from the pandemic have capitalized on scarcity to peddle fake vaccines and sell millions of counterfeit N95 masks and other personal protective equipment to health care facilities desperate to protect frontline workers. They have inflated their payrolls to obtain loans larger than they were eligible to receive. They have used shell companies and received assistance that they unlawfully diverted. They have set up operations to submit identical loan applications in the names of multiple companies. And they have fraudulently misrepresented the products or services they sold to the federal government.*

Like the pandemic itself, which has dragged on for longer than many imagined, the DOJ’s efforts to pursue pandemic fraud through use of the FCA is likely to linger for years to come, with each new phase of the pandemic offering new opportunities for alleged fraud and abuse.
On the Horizon – What’s Next For SEC Enforcement of ESG Priorities?

Posted on March 8th, 2022 by Matt Miller

This is the eighth post in this year’s series examining important trends in white collar law and investigations. Our previous post discussed trends in False Claims Act enforcement. Up next: trends in Federal Cryptocurrency Enforcement in 2022.

Key Takeaways

- Sensitive to criticism of regulation through litigation, the SEC’s Enforcement Division has not pursued cases dealing with cutting edge ESG issues before the SEC decides what, if any, new ESG disclosure requirements to impose.
- Pressure from leading voices in both the private and public spheres will likely lead the SEC to adopt a set of standards public companies must follow in making ESG disclosures.
- While the SEC’s next step on ESG disclosure rules remains unclear, it is a good bet that the SEC will try to align with efforts underway by international standard-setting organizations to adopt a globally accepted ESG baseline reporting standard.

It was one year ago, in March 2021, that the SEC’s Enforcement Division created its ESG Task Force. The Task Force’s mission was to develop initiatives proactively identifying ESG-related misconduct. As we noted at the time, the ESG Task Force’s mandate raised questions. The term “ESG” is convenient shorthand for a collection of complex and distinct topics that – it can be fairly said – are not intuitive to all participants in the capital markets. The E, or environmental, relates to how a company deals with risks and opportunities related to climate, pollution and other environmental factors, and the company’s impact on the environment. The S, or social, concerns a company’s values and business relationships, including human capital topics like employee health and safety, as well as diversity and inclusion efforts. The G, or governance, refers to corporate governance issues, including the composition and diversity of the board of directors, political contributions, and policies to prevent bribery and corruption.

How could the Task Force aggressively pursue misconduct related to ESG disclosures, where SEC leadership acknowledged at the same time that the rules governing how companies disclose complex ESG risks and opportunities are, at best, less than clear, and at worst, non-existent in certain respects? At the same time the Task Force was formed, the SEC sought public comments on disclosure rules for public companies targeted to ESG. Until the SEC decided upon the disclosure regime it would put in place for ESG, wouldn’t public companies push back against aggressive enforcement efforts in this area, charging the SEC with regulating through enforcement?

As we have seen recently, the SEC has been sensitive to those concerns. In November 2021 remarks, Gurbir Grewal, Director of the SEC’s Division of Enforcement, noted that the SEC was “starting to hear the popular
refrain ‘regulation by enforcement’ in the context of ESG.” Pushing back against that “refrain,” Grewal emphasized,

There is nothing “new” about how the Task Force – or the Enforcement Division as a whole – investigates possible climate and ESG-related misconduct. As with any investigation, we look to make sure our current rules and laws are being followed. For issuers, this means that we apply long-standing principles of materiality and disclosure. If an issuer chooses to speak on climate or ESG – whether in an SEC filing or elsewhere – it must ensure that its statements are not materially false or misleading, or misleading because they omit material information – just as it would when disclosing information in its income statement, balance sheet, or cash flow statement.

Director Grewal went on to highlight two Enforcement cases, one from 2008 and the other from 2020, that while touching upon ESG matters, were essentially run-of-the-mill misleading disclosure cases where the companies in question took it upon themselves to make representations regarding ESG matters that were, it turns out, false. According to Grewal, these cases “demonstrate that the requirements that companies’ disclosures be accurate and not misleading ... are not new, and should be of surprise to no one.”

Grewal’s comments suggest that until the SEC settles on a final disclosure regime moving forward, the Enforcement Division is not going to pursue cases on the vanguard of ESG disclosure issues. So, where do things stand on new ESG disclosure rules at the SEC, and where is the SEC likely to come out on this question?

**SEC Implementation an ESG Disclosure Regime**

While not much has happened outwardly since the SEC announced the beginning of efforts to reassess ESG disclosure requirements, the momentum seems to favor the adoption of a uniform disclosure framework that would allow tailoring to fit industry specific needs. Senator Elizabeth Warren has implored the SEC to adopt industry specific standards mandating disclosure with respect to climate risks, arguing that the existing climate disclosure framework adopted in 2010, which relies on a basic materiality without specific disclosure guidance, does not go far enough.

Private sector actors have likewise called for the SEC to adopt a set of ESG disclosure standards. Many, including heavily influential BlackRock, have advocated the SEC to incorporate standards developed by private sector standard setters, similar to the SEC’s incorporation of financial reporting standards promulgated by the Financial Accounting Standards Board (FASB). There is no shortage of existing disclosure frameworks from which the SEC could choose. The CDP (formerly the Carbon Disclosure Project), the Climate Disclosure Standards Board (CDSB), the Global Reporting Initiative (GRI), the International Integrated Reporting Council (IIRC), the Sustainability Accounting Standards Board (SASB), and the Task Force on Climate-Related Financial Disclosures (TCFD) have all published standards intended to help companies enhance the quality of their ESG disclosures.

Deloitte & Touche LLP, a Big Four accounting and consulting firm which has emerged as a thought leader on ESG disclosure issues, has commented that the SEC should be mindful of efforts already underway to globalize the many existing ESG reporting frameworks. Deloitte, and others, have noted the efforts of the International Financial Reporting Standards (IFRS) Foundation in establishing an International Sustainability Standards Board (ISSB) to adopt a globally accepted baseline for sustainability reporting standards. The IFRS Foundation’s influence in financial reporting is undeniable. It oversees the International Accounting Standards Board, which has promulgated financial reporting standards adopted by 140 jurisdictions across the world. Adhering to a
global framework developed by the ISSB could allow companies to avoid the inefficiencies and uncertainties of having to meet multiple and sometimes conflicting reporting standards across different jurisdictions.

The SEC has previously signaled its support of efforts to converge the various existing standards into a global baseline framework like the one being developed by the ISSB. Indeed, in a recent article, a trustee of the IFRS Foundation noted that the SEC was actively involved in the technical readiness working group supporting the development of ISSB standards. No matter the next step the SEC decides to take on ESG reporting and disclosure requirements, it is a good bet that the SEC will have in mind ways to align with efforts already underway to converge existing standards into one framework that public companies can rely on to meet various international reporting requirements. Until the SEC settles on an ESG disclosure regime, it appears likely that the Enforcement Division, as it has thus far, will continue to take a conservative view of its mandate to pursue cases in the ESG domain.

---

**Federal Cryptocurrency Enforcement in 2022**

Posted on March 11th, 2022 by Christopher Escobedo Hart and Yoni Bard

This is the ninth post in this year’s series examining important trends in white collar law and investigations. Our previous post discussed trends in SEC enforcement of ESG priorities. Up next: Looking at the Landscape of Congressional Investigations in 2022.

In 2021, various federal entities took steps toward establishing and exerting their enforcement authority against businesses and individuals transacting in cryptocurrency (or “crypto”), a digital asset that allows for decentralized transactions (i.e., no bank). As market participation continues to surge in this new asset class, big questions remain: What are the rules? Who is enforcing them? The combination of regulatory ambiguity, increased governmental scrutiny, and the multitude of different government actors that have staked out territory in crypto regulation is likely to yield a high level of cryptocurrency enforcement in 2022.

Key takeaways:

- There will likely be increased enforcement in 2022 against businesses and individuals involved in cryptocurrency.
- Cryptocurrency will remain a priority of the SEC, which continues to view this growing asset class with a high level of suspicion.
- The DOJ, now with a specialized cryptocurrency enforcement team, is expected to ramp up prosecution of crypto-related offenses with the support of the FBI’s new cryptocurrency unit.
- President Biden’s executive order on digital assets is a historic step by the federal government to take a unified approach toward cryptocurrencies, though the order calls for careful study before any regulatory action will be taken.
Despite the increased focus on cryptocurrency by the federal government, its status—as a security, a commodity, a currency, or something else—remains unclear, as does the applicable regulatory framework.

SEC and CFTC: the Lead Crypto Regulators

The key question in crypto enforcements is whether a cryptocurrency product or technology is a security (regulated by the SEC), a commodity (regulated by the CFTC), a currency (regulated by the Treasury Department), or something else.

Independent federal agencies have played the most active role in crypto enforcement. The U.S. Securities and Exchange Commission (SEC) has for years brought enforcement actions against entities making initial coin offerings or engaging in other cryptocurrency transactions based on theories of fraud or failure to register with the SEC. SEC Chair Gary Gensler, as we recently noted, has repeatedly highlighted cryptocurrency as an enforcement priority based on his views that the crypto market is rife with fraud and lacking in investor protection.

In 2022, the SEC will continue to crackdown on crypto entities that it considers to be dealing in securities, rather than using crypto technology for some other purpose, such as a medium of exchange. Chair Gensler has insisted that “each token’s legal status depends on its own facts and circumstances” based on a test devised by the U.S. Supreme Court for determining what counts as an “investment contract.” See SEC v. Howey Co., 328 U.S. 293 (1946). The SEC’s application of this 76-year-old test risks unpredictability and poses other challenges to cryptocurrency businesses looking for concrete guidance on how to achieve regulatory compliance.

Consider Coinbase, the cryptocurrency exchange that cancelled the launch of a crypto lending product in September after the SEC threatened the company with litigation. Or Ripple Labs, the payment technology company that the SEC sued in 2020 for selling cryptocurrency in what allegedly constituted an unregistered securities offering. This lawsuit, considered a test case for the SEC’s expansive classification of cryptocurrencies as securities, is expected to conclude in 2022.

The Commodity Futures Trading Commission (CFTC) has also been targeting cryptocurrency businesses since deciding in 2015 (here and here) that virtual currencies are commodities and therefore subject to CFTC jurisdiction.

The CFTC will continue targeting platforms offering cryptocurrency derivatives based on theories that those companies have engaged in unlawful commodity transactions or failed to register with the CFTC. In September, the CFTC announced a settlement order with Kraken, one of the largest cryptocurrency exchanges in the United States, for offering retail commodity transactions in Bitcoin and other cryptocurrencies, and for its failure to register as a futures commission merchant (a broker, essentially). The following day, the CFTC announced that it had initiated administrative proceedings against an additional 14 entities, most of which it claimed did not register as futures commission merchants. More settlement orders followed in October, as the CFTC collected over $42 million from Tether, which offers a cryptocurrency backed by the U.S. dollar (a “stablecoin”) and Bitfinex, a cryptocurrency trading platform.

The CFTC wants more. Last month, CFTC Chairman Rostin Behnam, in testimony before the Senate Agriculture Committee, suggested that Congress should expand the agency’s jurisdiction and increase its budget by $100 million to allow it to play a more key role in crypto enforcement.
Law Enforcement by Executive Departments

Regardless of whether a crypto product is treated as a security or a commodity, it may be subject to enforcement by various executive agencies, in particular, the U.S. Department of Justice (DOJ). In October of 2021, the DOJ announced the creation of the National Cryptocurrency Enforcement Team (NCET), a group including cybersecurity and money laundering prosecutors tasked with targeting “criminal misuses of cryptocurrency, particularly crimes committed by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors.” The NCET’s first Director, Eun Young Choi, has experience with cyber, fraud, and money laundering crimes, including those involving cryptocurrency.

Crypto-related enforcement is not new territory for the DOJ, which (as we recently noted in our tax post) last month announced a record-breaking seizure of over $3.6 billion of Bitcoin and the indictment of a married couple for their alleged role in laundering cryptocurrency stolen during the 2016 hack of the cryptocurrency exchange Bitfinex. The NCET, however, consolidates and organizes the DOJ’s crypto expertise into one unit that will pursue its own cases while supporting cryptocurrency investigations and prosecutions across the entire Criminal Division, and at the state and local levels. We expect that in 2022 (and beyond) the DOJ will flex this new enforcement group, leading to an increase in investigative activity against potential targets and witnesses in alleged crimes involving cryptocurrency. And with the DOJ’s recent announcement that the Federal Bureau of Investigations is also creating a specialized crypto team (the Virtual Asset Exploitation Unit), the DOJ will be even more equipped to step up its crypto prosecutions.

The U.S. Department of the Treasury, though historically not very involved in cryptocurrency regulation, is now attempting to bring some order to the growing use of this digital asset in foreign and international transactions. Its Office of Foreign Asset Controls (OFAC) has been primarily concerned by the prospect of entities or individuals using cryptocurrency to circumvent sanctions. As we explained in November, OFAC published guidance to assist the cryptocurrency community with OFAC compliance in the wake of cryptocurrency-related enforcement actions by the agency, which included adding a cryptocurrency exchange to its list of Specially Designated Nationals and Blocked Persons. On March 1, 2022, the Treasury Department issued a report in which it notes that cryptocurrency exchanges must follow the same Bank Secrecy Act rules as banks, which include registering with the Financial Crimes Enforcement Network (FinCEN) and having a chief compliance officer.

There is pressure on the Treasury Department to step up its enforcement. On March 2, 2022, several U.S. Senators sent a letter to the Treasury Department expressing concern that OFAC’s current crypto enforcement procedures do not adequately prevent bad actors from using cryptocurrency-tools to evade sanctions. The Senators emphasized the urgency of this issue, citing reports of Russia’s plans to soften the blow of U.S. sanctions by resorting to cryptocurrency transactions, which do not run through banks. The Senators concluded the letter by posing various questions to the Treasury Department to be answered no later than March 23.

Also within the Treasury Department, the Office of the Comptroller of the Currency (OCC) has recently focused on the increasingly popular stablecoins, the value of which is pegged to a national currency or a particular commodity, like gold. The Treasury Department seems to view this less volatile form of cryptocurrency with cautious optimism. As noted in a November report from the President’s Working Group on Financial Markets, “[i]f well-designed and appropriately regulated, stablecoins could support faster, more efficient, and more inclusive payments options.” Finally, last year FinCEN announced the addition of its first Chief Digital Currency Advisor, as this bureau of the Treasury Department continues to focus on the prevention and detection of illicit financial transactions.
Some Lawmaking by Congress

In addition to this frenzy of crypto activity from the Executive Branch, Congress recently enacted legislation that will apply reporting requirements to certain cryptocurrency transactions. Contained in the 1,039-page Infrastructure Investment and Jobs Act, signed into law by President Biden on November 15, 2021, are three pages of law that extend to digital asset transactions the existing reporting requirements (and tax collections) that apply to cash transactions over $10,000 and transactions involving a broker. These new reporting requirements, which will not take effect until 2024, may have the unintended consequence of deterring certain consumers and businesses from transacting in cryptocurrency. In the meantime, the U.S. Secretary of Treasury and the Internal Revenue Service have an opportunity to issue regulations to clarify the scope of these requirements.

Lingering Confusion

Despite these developments, Congress and regulators continue to draw criticism from the industry and government officials for failing to provide clear guidance to those wishing to engage in lawful cryptocurrency transactions. Some say the current regime looks more like regulation by enforcement. One outspoken critic of cryptocurrency’s regulatory ambiguity is Dawn Stump, a CFTC Commissioner who, through concurring statements (like this one, this one, and this one) and interviews, has discouraged the CFTC and the SEC from bringing enforcement actions against cryptocurrency businesses without first providing them with a clear regulatory framework.

Even members of Congress have criticized the regulatory void in which agencies are bringing enforcement actions. In a hearing before the Senate Banking Committee in September, Senator Pat Toomey (R-PA) expressed frustration to Chair Gensler regarding “the lack of helpful SEC public guidance” to determine which cryptocurrencies are securities and thus subject to the SEC’s jurisdiction.

President Biden’s Executive Order Seeks Federal Alignment

On March 9, 2022, President Biden issued his highly anticipated Executive Order on Ensuring Responsible Development of Digital Assets. The executive order recognizes the tremendous growth of cryptocurrencies and the various opportunities that they present, while acknowledging that the federal government needs to align its approach to maximize the potential benefits, and reduce the risks, of cryptocurrencies.

The policy objectives in the executive order are vast, extending from consumer and investor protection, to financial stability and global leadership, and even to human rights and climate change. While the order does not implement any immediate changes to cryptocurrency regulation, it calls for an in-depth review of the problems and promises of cryptocurrency by a laundry list of federal agencies with the goal of synchronizing and advancing the federal government’s oversight. The executive order, which was generally well-received by the crypto industry, marks the very beginning of the federal government’s first attempt to take a unified approach toward cryptocurrency.

So many signs point to an increase in crypto enforcement in 2022 as various government actors, with their respective remits and tools, pursue perceived misconduct involving this new asset class. President Biden’s executive order is a major step toward the adoption of a clear and comprehensive regulatory framework that seems likely to clear away some of the legal uncertainty that has surrounded cryptocurrency in the United States. In the meantime, cryptocurrency issuers, platforms, and funds will continue to face difficult decisions as they try to remain competitive in this growing industry while steering clear of government enforcement.
Looking at the Landscape of Congressional Investigations in 2022

Posted on March 16th, 2022 by Veronica Renzi, Austin A.B. Ownbey, Yoni Bard and Patrick Brennan

This is the tenth and final post in this year’s series examining important trends in white collar law and investigations. Be on the lookout for a roundup of our 2022 White Collar Year in Preview Series shortly.

Last March, we anticipated that the 117th Congress would use the powerful investigative tools at its disposal to drive its legislative agendas. Since then, we have seen congressional inquiries focusing especially intensely on climate change and prescription drug costs. This coming year, these two legislative priorities for the Biden Administration and Congress will continue to be the primary, but hardly the only, driver of congressional investigations.

The highest profile investigation on the Hill right now remains the Select Committee inquiry into the events of January 6, where, with the exception of some inquiries to social media companies, the private sector has not been a focus. But with many of Congress’s other investigative priorities, private sector entities are the chosen targets, and these investigations attract plenty of attention in their own right.

Looking back at the past year and at the possibility of shifting control in this fall’s midterms, here’s what we can expect from congressional investigations of the private sector in 2022:

• Congressional interest in climate change and health care costs, especially drug pricing, will continue to be intense, reflecting their importance to the Democrats’ legislative agenda.
• Debates over large technology companies and social media platforms will continue to be of great interest to Congress, with new areas of inquiry in 2022, like youth mental health.
• Investigations of the COVID-19 pandemic have largely focused on the government response, but the House Select Subcommittee on the Coronavirus Crisis has examined several health care providers and countermeasure manufacturers, and may expand its scope to more private sector actors and the broader economic effects of the pandemic.
• With rising inflation driving headlines over the past year, congressional committees began investigating pricing practices and market concentration in several industries. We expect such headline issues to continue to draw congressional attention.

Let’s take a closer look at these and other areas of congressional investigations.
Keeping Up the Pressure on Drug Pricing

Congress can be expected to keep the pressure on the pharmaceutical industry in 2022, building on several years’ worth of work to drive this year’s legislative efforts. This past December, the House Oversight Committee released a final staff report that summed up nearly three years of investigative efforts into pharmaceutical companies, citing findings that Medicare negotiations like those contained in the House-passed Build Back Better legislation could save the federal government billions of dollars.

Congressional focus on the pharmaceutical industry extends beyond pricing practices. Over the past six months, Hill leaders have expressed interest in reviewing the use of accelerated drug approvals by the Food and Drug Administration (FDA). Congress can shape policy in this area through the Prescription Drug User Fee Agreement (PDUFA) reauthorization process, due this year. FDA’s use of accelerated review was a popular topic at the first hearing on PDUFA in February, with Representative Jan Schakowsky (D-IL) forcefully arguing “we need to look at accelerated approval.”

Climate Change Efforts Heat Up

As part of legislative efforts on climate change, Congress has been investigating the fossil fuel industry on multiple fronts, with a stated commitment to large, long-term investigations of issues from allegations of climate change misinformation to assessments of companies’ clean energy pledges.

In October, the House Oversight Committee brought executives of four large oil companies to the Hill for a hearing that Committee Chair Carolyn Maloney (D-NY) compared to 1994’s congressional hearings with major tobacco executives. Maloney announced that the committee would be serving the companies with subpoenas following the hearing, later accusing the companies of having answered the Committee’s voluntary document request with “largely . . . non-substantive, publicly available materials, such as press clippings, regulatory filings, and pages from the entities’ own websites.” In February, the Committee held another hearing examining the same four companies, focused on their pledges to increase investments in clean energy.

Although a subsequent hearing with board members from the same companies was canceled, there is no sign of Congress’ interest in these companies relenting, especially with oil prices increasing. Representative Maloney made her intentions clear in January, saying, “We’ve only begun our investigation into the fossil fuel industry’s role in causing the climate crisis and spreading disinformation.” As oil prices have risen rapidly amidst the war in Ukraine and sanctions on Russia, oil and gas companies may come under scrutiny about pricing and other policies this year as well.

A New Bipartisan Focus in Big Tech Investigations

Large technology companies, especially social media platforms, continue to attract passionate bipartisan interest. In September, bipartisan subcommittee leaders Richard Blumenthal (D-CT) and Marsha Blackburn (R-TN) announced an investigation into social media’s harms to youth, based on the Wall Street Journal’s reporting that companies had hidden information on the issue. The subcommittee has now held two hearings with four tech executives on the topic, and in November, the House Oversight Committee requested information from TikTok about practices that may be harmful to youth. Given the existing bipartisan interest and the progress on bipartisan tech legislation, this is likely to remain an area of intense investigation even if control of Congress shifts in the midterm elections.
Although Republicans lack the power to issue subpoenas unilaterally, members in the minority have also made clear some of their own areas of interest. In February, they wrote to Oversight Chair Carolyn Maloney to request a committee hearing on GoFundMe’s decisions around fundraisers for the Canadian trucker convoy, and the minority members wrote separately to GoFundMe requesting documents. The Committee majority also launched an investigation into technology companies’ role in the convoy, requesting information from Facebook about coordination on the platform.

COVID-19 Oversight Continues

Congressional investigations regarding the COVID-19 pandemic have generally focused on federal agencies rather than private actors, but one ongoing area of scrutiny for the private sector is the Paycheck Protection Program (PPP), which made more than $900 billion in potentially forgivable loans to businesses. Last year, the Select Committee on the Coronavirus Crisis sent letters requesting information from six different financial technology firms, pointing to reports that the firms were “linked to a disproportionate number of PPP loans made to fraudulent or ineligible applicants.” That investigation has not yet concluded, and the White House’s announcement of stepped-up enforcement against pandemic fraud could drive continuing congressional interest.

Additionally, the Committee has expressed an interest in investigating misinformation around COVID-19 treatments, requesting records from telehealth companies on the issue. Last year, the Committee also investigated vaccine production by the federal contractor Emergent BioSolutions, which involved requesting information first from Emergent and then Emergent partners Johnson & Johnson and Pfizer. In December, the Committee released its Emergent findings, as well as findings of an investigation into primary care provider One Medical’s practices around vaccine prioritization. Potentially revealing a broader focus for 2022, the Select Committee recently launched one of its first investigations into the broader economic effects of the pandemic, joining the House Oversight Committee in requesting information from three major shipping lines about high shipping prices during the pandemic.

Financial Innovation Draws Inquiries

Congressional committees with oversight of the financial industry have drawn attention in the past year to several areas of rapid change, including the development of Special Purpose Acquisition Companies (SPACs) and the growth of cryptocurrencies. In September 2021, four Democratic senators on the Banking Committee requested information from six firms that work on SPAC transactions requesting information on the deals they had led. This may be just the beginning of congressional interest in SPACs, with the senators stating that the inquiry will inform “what sort of Congressional or regulatory action” is appropriate for the industry.

Amidst turbulent cryptocurrency prices and calls for Congress to regulate the growing industry, the House Financial Services Oversight Subcommittee brought executives of major cryptocurrency companies to the Hill last July. Citing the work of the Biden Administration’s Working Group on Financial Markets, Senate Banking Committee Chair Sherrod Brown (D-OH) issued requests for information from eight different companies that work with “stablecoins,” cryptocurrencies tied to other commodities or currencies. Over the past several months, both the Banking Committee and the House Financial Services Committee have held hearings with stablecoin experts and industry leaders, including one CEO who was also subpoenaed in October by Securities and Exchange Commission. During the Banking Committee hearing, Senator Brown noted cryptocurrency companies’ high-profile TV advertisements during this year’s Super Bowl, indicating significant and continuing congressional interest in the industry more broadly.
Investigating Inflation and Cost of Living Concerns

As meat prices rose substantially over the past two years, cattle ranchers and other meat producers worked to draw attention to concentration and purchasing practices in the meatpacking industry. The Senate Judiciary Committee brought top meatpacking executives to Congress for a hearing in July 2021, while the House Oversight Subcommittee on Economic and Consumer Policy requesting pricing information from them this January.

In our blog post last March, we noted that Congress was using investigations to build a case for antitrust reforms, and we expect that Congress will continue citing inflation, supply chain concerns, and rising consumer prices as part of these broader efforts, as they have with meatpacking already.

While Republican members of Congress have shown significant interest in inflation concerns, some have also criticized their Democratic colleagues’ priorities and proposed focusing instead on regulations by the Biden administration—a harbinger of potential priority areas if they were to retake the House.

Separately, Democrats in the House and Senate have also been probing pricing practices and other issues tied to private equity investment. In March 2021, the House Ways and Means Oversight Subcommittee held a hearing on the role of private equity in health care, followed by the subcommittee’s chair, Bill Pascrell (D-NJ), requesting that the Government Accountability Office examine private equity’s role in the industry. The Senate Banking Committee and Senator Elizabeth Warren (D-MA) have requested information from companies regarding private equity’s influence in other industries as well, including housing and manufacturing.

Ongoing Scrutiny for Organ Procurement Organizations

Last July, as part of a webinar on how to navigate congressional investigations, we looked at the case study of organ procurement organizations (OPOs), nonprofit organizations that receive federal contracts to allocate the nation’s supply of organs. This area has been a focus both for Congress and the executive branch, with the Trump Administration finalizing and the Biden Administration now implementing new standards to incentivize better OPO performance. Since our webinar, the investigation continues to attract media attention for the OPOs under the most intense scrutiny, and members such as Representative Katie Porter (D-CA) have cited media reports to emphasize the need for continuing investigation in 2022.

Conclusion

We expect that many of the investigations described above will continue in some form even with a change in control of Congress this fall. As Republicans hope to win back the House of Representatives—and therefore subpoena power—in the midterm elections, they may begin laying the groundwork for investigative efforts with more information requests this year. Companies should be looking not only to existing areas of congressional focus, but also major news stories, media investigations, executive branch actions, and the parties’ broader political priorities to know where Congress may turn its investigative attention next.
The Foley Hoag White Collar Law & Investigations blog addresses the developing regulatory environment that confronts businesses and individuals in virtually any industry. Whether federal or state investigations, enforcement actions, changing enforcement priorities, criminal prosecutions or related civil proceedings, the White Collar Law & Investigations blog will provide regular coverage and updates that draw on the deep experience of Foley Hoag's White Collar Law & Investigations practice.