FOLEY HOAG

FOLEY HOAG 2024 WHITE COLLAR YEAR IN PREVIEW SERIES

foleyhoag.com

FOLEY HOAG

Foley Hoag 2024 White Collar Year in Preview Series

FOLEY HOAG LLP

TABLE OF CONTENTS

HEALTH CARE FRAUD ENFORCEMENT IN 2024

by Caroline Donovan, Yoni Bard and Jace Lee

The government had another busy year in 2023, investigating and prosecuting healthcare fraud cases on multiple fronts. Contending with the enormous healthcare crises of the now-concluded COVID-19 pandemic and the ongoing opioid epidemic, the government has deployed considerable resources to combat allegedly fraudulent schemes that have resulted in financial loss to the government and individual harm. Meanwhile, new technology has shifted the enforcement landscape, with the government targeting telemedicine fraud and relying ever-increasingly on data analytics to identify suspected outliers associated with potential fraud.

But the government's most powerful tool for combating health care fraud remains, as always, the False Claims Act (FCA). In 2023, we saw an unprecedented number of investigations and settlements, as well as significant case law developments. We expect to see similar priorities and enforcement levels as we examine healthcare fraud enforcement in 2024.

Covid-19 Pandemic Fraud

Though some years have passed since the height of COVID-19, the government has not slowed down in bringing enforcement actions related to the pandemic. In fact, at the recent Federal Bar Association's Qui Tam Conference on February 22, 2024, Assistant Attorney General Brian M. Boynton stated that COVID-19 fraud has been, and will continue to be, an FCA enforcement priority this year. In particular, Boynton stated that the key focus will be on fraud involving the Paycheck Protection Program (PPP), which provided loans to eligible small businesses for payroll, rent, utility payments, and other business-related costs. Corroborating these remarks, DOJ recently announced in a press release on February 22, 2024, that, among its record-breaking number of FCA settlements and judgments in 2023, DOJ has resolved approximately 270 FCA matters involving the PPP loans, amounting to nearly $48.3 million of recovery to the government. Many of these cases involved small businesses and individuals who used PPP loans in unauthorized ways, such as purchasing luxury items and sports cars.

Beyond fraud involving PPP loans, other pandemic-related fraud will likely remain an enforcement priority. In the November 2023 annual report by the Health Care Fraud and Abuse Control (HCFAC) Program, the government identified additional pandemic-related fraud schemes, including clinics offering "unnecessary services" to patients, in addition to COVID-19 tests, in exchange for the patients' personal information that they then use to fraudulently bill federal health care programs for those unnecessary services; performing "unnecessary laboratory testing" and billing those tests along with Covid-19 tests; making false and fraudulent representations about Covid-19 testing, treatments, or cures; and fraudulently obtaining Covid-19 health care

relief funds, such as by making false claims and/or submitting fraudulent applications. Similarly, the DOJ's press release on February 22, 2024, noted such cases as key FCA settlements and judgments in the last fiscal year. The government has not concluded its enforcement work arising from the pandemic and alleged fraud associated with it, and we expect to see robust COVID-19-related enforcement in 2024 as the dust settles after an unprecedented public health crisis.

Opioid Enforcement

Opioid enforcement continues to be a priority for the government among its various healthcare fraud initiatives. DOJ's Fraud Section heads up the Prescription Strike Force, which in the past six years, together with the New England Prescription Opioid (NEPO) Strike Force, has charged over 120 defendants for illegally prescribing nearly 120 million controlled substance pills that were medically unnecessary. As of February 2024, more than 85 of those defendants had been convicted.

In April 2023, a Tennessee jury convicted a nurse practitioner – known locally as the "Rock Doc" – on multiple counts of prescribing opioids, including oxycodone and fentanyl, outside the scope of professional practice and without a legitimate medical basis. And in June 2023, a Kentucky jury returned a guilty verdict against a dentist for unlawfully prescribing opioids for routine dental procedures, including morphine that caused the death of one of his patients. A few days later, DOJ announced a two-week nationwide law enforcement action, coordinated with federal and state law enforcement partners, that resulted in criminal charges against 24 physicians and other healthcare professionals for their alleged participation in opioid abuse schemes.

As the nation's unprecedented opioid crisis continues to unfold, we expect that the government will keep leveraging its strike forces and other resources to pursue healthcare providers for their alleged role in unlawfully supplying these drugs.

Telemedicine Fraud

We anticipate that telemedicine fraud will be another top enforcement area in 2024. On February 26, 2024, the DOJ's Health Care Fraud Unit (HCFU) issued an annual Year-in-Review report for the last fiscal year, identifying telemedicine fraud as a priority. It explained that, since the onset of the Covid-19 pandemic, fraud schemes utilizing telemedicine have "exploded." These fraud schemes allegedly involve call centers and marketers often targeting the elderly and disabled populations through either predictive dialers or direct mail, television, internet, and other forms of advertising. These purported marketers then "upsell" to these vulnerable populations unnecessary durable medical equipment, medical testing, prescriptions, and other items and gather personal information to draft doctors' orders without the input of trained medical professionals or staff. Telemedicine companies then offer remuneration to doctors or nurses to sign these orders without any in-person patient interaction or with only a brief telephonic conversation. Medical equipment companies or laboratories ultimately use these signed orders to submit fraudulent claims to Medicare and other health insurance plans. The HCFU stated in its report that its prosecutions "aim to provide full-spectrum accountability of actors at all levels of these conspiracies."

Consistent with the report above, DOJ has brought major telemedicine fraud actions in recent years and will likely continue to do so. As recently as February of this year, the U.S. Attorney's Office for the District of Massachusetts announced in a press release that it prosecuted the owner of Expansion Media (Expansion) and Hybrid Management Group (Hybrid), who pleaded guilty in connection with a $110 million telemedicine

fraud scheme involving medically unnecessary durable medical equipment, including orthotics such as back and knee braces. The fraud scheme essentially falls within the pattern described above, where, in exchange for kickbacks, the owner of Expansion and Hybrid assisted telemedicine companies obtain signatures by doctors and nurses for fraudulently generated orders without performing a legitimate examination of Medicare beneficiaries. Notably, this prosecution reflects a continuation of the telemedicine enforcement trend from last year, where the DOJ engaged in a major two-week national campaign that brought criminal charges against 78 defendants for alleged participation in healthcare fraud, including against corporate executives of the telemedicine companies as well as licensed physicians who signed these fraudulent orders.

Increasing Use of Data Analytics

While relators (or "whistleblowers") continue to be the primary fuel for FCA enforcement, DOJ is increasingly turning to data analytics to identify potential fraud by looking at outliers in healthcare reimbursement data. The HCFU, which prosecutes complex healthcare fraud cases, touts its "team of dedicated data analysts [that] work with prosecutors to identify, investigate, and prosecute cases using data analytics." In its 2023 recap, DOJ's Fraud Section noted that the HCFU's Data Analytics Team fulfilled nearly 3,000 data requests and proactively made over 200 investigative referrals.

It's no wonder that data analytics played a role in significant convictions and settlements. In one case, the HCFU used data analytic tools to identify suspected fraud related to the CARES Act Provider Relief Fund, revealing that certain individuals had no COVID-19-related expenses and misappropriated the funds for personal expenses. As of February 2024, 12 of the 14 defendants charged for this conduct had been convicted. Another example involved Medicare billing for respiratory pathogen panel (RPP) testing in conjunction with COVID-19 billing where RPP testing was not medically necessary. The Los Angeles-based Health Care Providers Lab (HCPL) stood out in data analysis as "an extreme outlier for billing the CPT codes for RPP testing," almost always combining these with codes for COVID-19 testing. The data also revealed clusters of patients in the same area and large numbers of patients referred to the lab by the same physicians. Through an HCFU investigation, the government determined that the lab had been obtaining nasal swab specimens from various patients in group settings (e.g., assisted living facilities, rehabilitation facilities, primary and secondary schools) for Covid-19 testing but had been running RPP tests on some of the specimens without medical justification, resulting in around $360 million in fraudulent claims to Medicare and other insurers for RPP tests and around $54 million in reimbursements to the lab. The owners of the lab, a husband and wife, both pleaded guilty.

In a September 30, 2023, press release, DOJ revealed a $172 million settlement by Cigna Group to resolve FCA allegations. The settlement related to allegations of fraudulent billing to Medicare Advantage (also known as Medicare Part C), which last year became the largest component of the Medicare program based on the number of beneficiaries and federal spend. According to DOJ, Cigna submitted false diagnosis codes on claims for its Medicare Advantage plan members, reporting "diagnoses of serious and complex conditions" without proper diagnostic tools and to "increase its Medicare Advantage payments by making its plan members appear sicker." The U.S. Attorney's Office for the Eastern District of Pennsylvania, in connection with this settlement, stated that it is prioritizing the investigation of fraud involving Medicare Advantage, given its growth, and that the Office employs "data-driven investigative methods" as part of its investigations.

We can expect data analytics to play an increasingly larger role in the government's investigation and prosecution of health care fraud, particularly as analytical tools and artificial intelligence continue to become more sophisticated.

False Claims Act Enforcement

As we noted in our recent FCA post, 2023 was a big year for the False Claims Act. The government resolved a record-breaking number of FCA matters, and significant FCA decisions continued to shape the future of FCA enforcement. Health care has long been, and will continue to be, a key area of FCA enforcement for the government and the primary source of FCA settlement payments (in 2023, roughly 70% of all FCA settlement proceeds). Within health care, the government remains focused on financial inducements for referrals (also associated with charges under the Anti-Kickback Statute and the Stark Law prohibiting self-referrals) and unlawful laboratory referrals, among other alleged schemes.

We first look at the numbers. On February 22, 2024, when he spoke at the Federal Bar Association's Qui Tam Conference regarding healthcare fraud enforcement in 2024, Principal Deputy Assistant Attorney General Boynton highlighted the following metrics from 2023:

- It marked the 15th consecutive year that DOJ's FCA recoveries exceeded $2 billion (they almost reached $2.7 billion);
- DOJ had record-setting performance, scoring 543 FCA settlements and judgments;
- DOJ investigated 712 qui tam lawsuits – the third-highest yearly total in the FCA's history;
- DOJ complemented its qui tam cases by opening more than 500 FCA cases that were not qui tams; and
- DOJ's Fraud Section issued 1,504 Civil Investigative Demands, marking another all-time record.

The FCA activity we are seeing lately also includes cases predicated on violations of the Stark Law (prohibiting physician self-referrals). On October 10, 2023, DOJ announced an $85.5 million settlement with Cardiac Imaging Inc. to resolve allegations that the mobile cardiac PET scan provider and its founder paid kickbacks to cardiologists by giving them above-market supervision fees to induce patient referrals for PET scans, thereby violating the Anti-Kickback Statute (AKS) and the Stark Law. DOJ later went after the company's former president and CFO, announcing on February 5, 2024, the unsealing of a complaint against the former executive for playing a pivotal role in the scheme.

On December 19, 2023, DOJ published a press release regarding the largest-ever FCA settlement based on Stark Law violations. The Indianapolis-based Community Health Network Inc. agreed to pay $345 million to resolve allegations that it paid various physicians, including cardiologists and certain surgeons, compensation above fair market value, awarded bonuses to physicians based on their number of referrals, and submitted claims to Medicare based on these referrals. The settled litigation arose from a whistleblower complaint filed in 2014 by the company's former CFO and COO.

Amidst a busy year for FCA enforcement, the Supreme Court issued two significant FCA decisions in the summer of 2023. The first, *United States, ex rel. Polansky v. Executive Health Resources, Inc.*, 599 U.S. 419 (2023), addressed the timing and standard of review for the government to dismiss an FCA case over a relator's objection. The Court concluded that the government may dismiss a case so long as it intervened at some point

in the litigation, whether during the initial seal period or subsequently after showing good cause for an initial declination. The Court also clarified that district courts, when reviewing a motion to dismiss by the government, should apply the ordinary voluntary dismissal standards set forth in Rule 41(a) of the Federal Rules of Civil Procedure. It remains to be seen whether the *Polansky* decision will have an impact on the frequency with which the government pursues voluntary dismissals.

In the second, *United States ex rel. Schutte v. SuperValu Inc.* and *United States ex rel. Proctor v. Safeway, Inc.*, 598 U.S. 739 (2023), the Court considered a pair of consolidated cases regarding the FCA's scienter requirement and unanimously held that defendants cannot avoid FCA liability by demonstrating that their conduct was consistent with an "objectively reasonable" interpretation of an ambiguous legal requirement. The relevant inquiry, the Court clarified, is the defendant's knowledge (whether actual or constructive) and subjective beliefs at the time the defendant submitted the allegedly false claim. This decision will likely have at most a modest impact on the trajectory of FCA investigations and litigations, given the unique facts in these cases and the government's – and courts' – longstanding focus on a defendant's subjective belief as the relevant metric of scienter. For a further analysis of lower courts' application of these decisions, please see our recent FCA post.

The Supreme Court has not been the only court to issue significant FCA decisions lately. In March 2024, the U.S. Court of Appeals for the Second Circuit addressed the type of knowledge a relator must prove to prevail in an FCA claim based on an Anti-Kickback Statute (AKS) violation. *See United States ex rel. Hart v. McKesson Corp.*, No. 23-726-cv, 2024 U.S. App. LEXIS 5857 (2d Cir. Mar. 12, 2024). The relator in this case filed a complaint against pharmaceutical wholesaler McKesson, asserting violations of the AKS and analogous state laws based on the company's alleged provision of valuable business management tools to physicians to induce them to purchase drugs from the company. The district court dismissed the AKS claim on the basis that the relator had not sufficiently pleaded the requisite level of scienter for an AKS claim, namely that the company had acted "willfully." Affirming the district court, the Second Circuit held that to act "willfully" for the purpose of an AKS violation, a defendant must have knowledge that its conduct is somehow unlawful, even if the defendant is not aware that the conduct specifically violates the AKS.

McKesson may raise the bar for some courts that were allowing relator's AKS claims to survive a motion to dismiss where the allegations did not satisfy the willfulness requirements articulated by the Second Circuit, and therefore spare defendants from litigating these cases or paying hefty sums to settle them.

FALSE CLAIMS ACT ENFORCEMENT: LOOKING BACK AND WHAT TO EXPECT IN 2024

by Caroline Donovan and Jasmine N. Brown

It is not often that we can say that a federal fraud statute had a blockbuster year. However, 2023 was exactly that for the False Claims Act ("FCA"). Not only did enforcement activity by the Department of Justice reach record-breaking numbers, but we also received long-awaited decisions from the Supreme Court in *United States, ex rel. Polansky v. Executive Health Resources, Inc.* and consolidated cases, *United States ex rel. Schutte v. SuperValu Inc.* and *United States ex rel. Proctor v. Safeway, Inc.*

2023 By the Numbers

Overall, the government's recoveries in fiscal year 2023 were up compared to 2022, with total dollar recoveries in 2023 increasing to $2.68 billion compared to $2.2 billion in 2022. Nevertheless, these numbers are down significantly from 2021, which saw False Claims Act recoveries totaling $5.6 billion.

The total dollars recovered belies, however, the record-breaking number of FCA matters that were resolved in 2023. The government and whistleblowers resolved 543 matters through settlements and judgments, the highest number of resolutions in a single year. This is a substantial increase over the 351 resolutions in 2022. Additionally, there was a steady increase in whistleblower actions, with 712 *qui tam* actions filed in 2023, averaging more than 13 new cases every week.

Healthcare Still Driving FCA Enforcement, But Trending in Other Sectors Continues

While the healthcare industry remained the predominant area of FCA enforcement, with more than $1.8 billion in total dollars recovered, other sectors, in particular cybersecurity, COVID-related fraud, customs and tariffs, small business contracting, and telecommunications, saw increased enforcement activity in 2023, as we had suggested may be the case last year.

Under the Civil Cyber-Fraud Initiative, the government settled two additional matters in 2023 for roughly $4.3 million. In both cases, the government alleged that the corporate entities failed to provide adequate cybersecurity protections in violation of their contract or contrary to the representations made in receipt of federal funds. In one of those matters, involving Verizon Business Network Services' $4 million settlement, the government credited the company for taking significant steps to cooperate with the government, including providing a written self-disclosure to the government and several supplemental disclosures, initiating and conducting an independent investigation, and conducting a compliance review of the alleged issues.

Moreover, in 2023, the government resolved approximately 270 matters and recovered over $48.3 million related to improper COVID-19 Paycheck Protection Program loan payouts. The government pursued recoveries for additional COVID-related fraud schemes, including schemes by healthcare providers to bill for unnecessary tests and services. As part of its stated commitment to hold individuals responsible as well as their companies, the government alleged that Patrick Britton-Harr and his lab companies offered COVID-19 tests to nursing homes as part of a scheme to bill Medicare for medically unnecessary respiratory pathogen panel tests that were not ordered by a treating physician.

As part of the same commitment to holding individuals accountable, Margarita Howard and her company, HX5 LLC, paid approximately $7.8 million to resolve allegations of a small business fraud scheme. The government alleged that Ms. Howard knowingly provided false information to the Small Business Administration regarding HX5's eligibility for federal set-aside contracts meant to go to small businesses owned and controlled by socially and economically disadvantaged individuals.

The government also settled a matter with the International Vitamins Corporation for $22.8 million for an alleged scheme of misclassifying certain vitamin and nutritional supplements to avoid paying customs tariffs and duties. As part of the settlement, IVC admitted that it did not correct the classifications for over nine months and did not remit the duties to the United States after being informed by its hired consultant that it was engaged in wrongful conduct. Finally, the GCI Communications Corporation paid $40 million after the government alleged that it received excess subsidies in connection with the Federal Communications Commission's Rural Health Care Program after it inflated its prices and violated the FCC's competitive bidding regulations.

We expect growth consistent with historical trends for recoveries, settlements, judgments, and new qui tam actions throughout 2024. We also expect continued enforcement in the government's recent areas of interest.

Key Decisions: *Polansky* and *SuperValu / Safeway*

Last year, we previewed two highly anticipated sets of decisions from the U.S. Supreme Court: *United States, ex rel. Polansky v. Executive Health Resources, Inc.,* concerning the government's ability to dismiss over the relator's objection, after declining to intervene, and the consolidated cases, *United States ex rel. Schutte v. SuperValu Inc.,* and *United States ex rel. Proctor v. Safeway, Inc.*, concerning the scienter requirement, namely whether a defendant acts knowingly when the defendant proffers an objectively reasonable interpretation of regulations, notwithstanding the defendant's subjective belief.

The Court's decisions in June 2023 resolved the questions presented: In *United States ex rel. Polansky v. Exec. Health Res., Inc.,* 599 U.S. 419 (2023), the Court held that the "Government may seek dismissal of an FCA action over a relator's objection so long as it intervened sometime in the litigation" and that such motions will be decided pursuant to Federal Rule of Civil Procedure 41(a) regarding voluntary dismissals. In addressing the latter question concerning the standard for dismissal, the Court was clear that while the False Claims Act requires notice and opportunity for a hearing before dismissal, "the Government's views are entitled to substantial deference" and that "[i]f the Government offers a reasonable argument for why the burdens of continued litigation outweigh its benefits, the court should grant the motion. And that is so even if the relator presents a credible assessment to the contrary."

In the consolidated cases, *United States ex rel. Schutte v. SuperValu Inc.*, *United States ex rel. Proctor v. Safeway, Inc.*, 598 U.S. 739 (2023), the Supreme Court held that the FCA's scienter element "refers to respondents' knowledge and subjective beliefs—not to what an objectively reasonable person may have

known or believed." Thus, even when faced with an ambiguous statute or regulation, "such facial ambiguity is not sufficient to preclude a finding that respondents knew that their claims were false." Rather, scienter is based on what the defendant thought when submitting the allegedly false claim.

Application of *Polansky* and *SuperValu / Safeway*

Since the Supreme Court's decision, each case applying *Polansky*'s holding has confirmed the government's dismissal authority. Among the small handful of cases decided in the 10 months since *Polansky*, the question of the standard has garnered some attention. In *Brutus Trading, LLC v. Std. Chtd. Bank*, the Second Circuit affirmed the district court's dismissal and interpreted what was required to satisfy the False Claims Act's hearing requirement. The Second Circuit found that "the district court met the hearing requirement by carefully considering the parties' written submissions" and that there was no due process violation because the relator did not show that the government's decision to dismiss was unreasonable or arbitrary. Other courts assessing the government's interests have likewise given deference to those interests, as required under *Polansky*. Thus, in *United States ex. rel. Erik K. Sargent v. McDonough*, No. 23-cv-328, 2024 U.S. Dist. LEXIS 32973 (D. Me. Feb. 26, 2024), the district court credited the government's argument that the burdens outweighed the benefits of litigation, especially where the government would be pursuing a $95,000 claim against a government agency (the Department of Veteran Affairs). And in *United States ex rel. USN4U, LLC v. Wolf Creek Fed. Servs.*, No. 17-cv-558, 2023 U.S. Dist. LEXIS 217620 (N.D. Oh. Dec. 7, 2023), the district court likewise found that dismissal was proper based on the government's arguments concerning the lack of evidence, unlikelihood of success, and burden even in monitoring the case.

As *Polansky* signaled and the cases decided since then have made clear, it will only be in the exceptional case that the government's motion to dismiss after intervention will be denied. We've yet to see that case.

Recent cases applying the holding in *SuperValu* and *Safeway* have also provided more color regarding the subjective belief scienter standard, including areas not covered by the Supreme Court's most recent holding. To that end, in *United States v. Peripheral Vascular Assocs.*, P.A., No. 17-cv-317, 2024 U.S. Dist. LEXIS 16689 (W.D. Tex. Jan. 30, 2024), the court held that the Supreme Court's decision did not fully dispose of an objective application in cases where the recklessness standard of scienter is applicable. The court, citing language in the footnotes of *SuperValu*, maintained that the objective standard may be utilized "[i]n some civil contexts," such as when "a defendant may be called 'reckless' for acting in the face of an unjustifiably high risk of illegality that was so obvious that it should have been known, even if the defendant was not conscious of that risk." Moreover, a handful of other cases have applied the Supreme Court's holding such that the petitioner does not have to present evidence of the respondent's actual, subjective knowledge that they were submitting a false claim but rather evidence sufficient to show an inference that the respondent's subjectively knew that they were submitting a false claim. *See United States v. McComber*, No. 21-cr-36, 2024 U.S. Dist. LEXIS 50974 (D. Md. Mar. 22, 2024) (noting that "nothing in *SuperValu* suggests that a defendant can bury its head in the sand and avoid FCA liability in the face of overwhelming evidence that its submissions to the Government contained false statements."). Finally, at least one court has refused to extend the holding to eliminate an objective scienter standard in other provisions of the FCA, such as § 3730, which governs protected activities such as retaliation.

Hennessey v. Mid-Michigan Ear, Nose & Throat P.C., No. 21-cv-301, 2023 U.S. Dist. LEXIS 125639 (W.D. Mich. July 21, 2023).

SEC TO CONTINUE AGGRESSIVE ENFORCEMENT EFFORTS IN 2024 AFTER RECORD-SETTING 2023

by Anthony D. Mirenda, Christopher Escobedo Hart, Leah S. Rizkallah, Yoni Bard, Christian Garcia, Rachel Kerner and Susanna Chi

The U.S. Securities and Exchange Commission's Enforcement Division resumed its dogged pursuit of investigations and enforcement actions in fiscal year 2023. The SEC announced that the Division initiated 784 total enforcement actions in 2023 (a 3% increase from fiscal year 2022), including 501 "stand-alone" actions (i.e., enforcement actions excluding those brought against issuers for delinquent filings and "follow-on" administrative proceedings seeking bars against individuals; an 8% increase from fiscal year 2022), 121 actions against issuers for delinquent filings (a 6% decrease from fiscal year 2022), and 162 "follow-on" administrative proceedings (a 26% increase from fiscal year 2022). Those enforcement actions spanned several notable subject areas, including insider trading, crypto asset securities, cybersecurity, recordkeeping, and actions to protect whistleblowers. The SEC collected $4.949 billion in financial remedies, representing the second highest amount in SEC history, including $3.369 billion in disgorgement and $1.580 billion in civil penalties. The SEC also obtained orders barring 133 individuals from serving as officers or directors of public companies – marking the highest number in a fiscal year in over a decade – and returned $930 million to harmed investors in fiscal year 2023.

The Commission's Whistleblower Program likewise enjoyed unprecedented success in fiscal year 2023. The SEC issued whistleblower awards totaling nearly $600 million, a record for the program and a substantial increase from the $229 million awarded in fiscal year 2022. The Commission also reported receiving more than 18,000 whistleblower tips (a nearly 50% increase over fiscal year 2022) and issuing a record-setting $279 million award to one whistleblower.

Further strengthening the Whistleblower Program, as we detailed in a recent Foley Hoag client alert, the Supreme Court eased the standard for establishing whistleblower retaliation claims in its February 8, 2024 decision in Murray v. UBS Securities, LLC. In this decision, the Court ruled that an employee can prove a whistleblower retaliation claim under the Sarbanes-Oxley Act without showing that his employer acted with retaliatory intent.

Fiscal year 2023 represented a continuation of the forceful regulatory stance the SEC has taken under Chairman Gary Gensler and Enforcement Director Gurbir Grewal. We expect the Commission to continue to aggressively pursue enforcement actions into fiscal year 2024 while focusing on the priorities discussed below.

Insider Trading Remains a Top Priority

As noted above, the fiscal year 2023 enforcement data shows that the SEC's focus on investigating and prosecuting insider trading remains steady. However, 2023 also brought some new developments to the SEC's historic theories of insider trading.

For example, a jury is now set to hear the SEC's first "shadow trading" case in *SEC v. Panuwat*. Shadow trading, a novel theory of insider trading liability, involves an investor possessing material non-public information about Company A, who trades in the securities of Company B, another company with which Company A shares some connection in the market (such as a competitor or comparable company). In *Panuwat*, the SEC alleged that Panuwat, the then-head of business development at Medivation (a mid-sized, oncology-focused biopharma company), purchased short-term, out-of-the-money stock options in Incyte Corporation (another mid-sized, oncology-focused biopharma company), just days before the August 22, 2016 announcement that Pfizer would acquire Medivation at a significant premium. According to the complaint, when he did so, he knew that investment bankers had cited Incyte as a comparable company in discussions with Medivation, and he anticipated that the acquisition of Medivation would likely lead to an increase in Incyte's stock price. In November 2023, the Northern District of California denied summary judgment to the defendant, Panuwat, over his objections that there was no evidence of ill-intent, that he was not on notice that his actions violated the insider trading prohibitions and that he should not be the test case for whether shadow trading can survive in court. The action, which seeks damages of $100,000 in profits from alleged "shadow" trades, will move ahead for trial scheduled in 2024. Given that this theory of liability survived summary judgment, we expect it to be employed in more cases in the coming year, particularly given that shadow trading activity is thought to be widely popular in the industry. Moreover, if the SEC prevails at trial, such a victory is likely to have huge precedential implications. That said, questions about the theory's scope remain. For example, even if the theory is successful in this case, it remains to be seen whether the theory can be successfully employed against trading in all unrelated companies across a sector or industry or whether the companies must be identical in focus and discussed as comparable in the market (as in *Panuwat*). The *Panuwat* trial and any related appeal may provide further guidance on how far this theory can stretch.

In another example, in the classic "tipping theory" case, a tippee's liability for insider trading is derivative of the tipper's liability, meaning a tippee is ordinarily not liable unless the tipper is also liable. In *US v. Klundt*, the SEC brought charges against individuals Sargent and Klundt for insider trading, alleging that Sargent purchased stock and options based on the material, non-public information he received from Klundt. In January 2023, following a multi-day trial, a jury found Klundt, the tipper, not guilty of insider trading, whereas Sargent, the tippee, was found guilty of the crime. Not surprisingly, Sargent challenged the verdict against him as inconsistent. The SEC then sought to uphold the conviction, arguing for tippee liability notwithstanding the seemingly inconsistent jury verdict. In December 2023, a judge ordered from the bench that Sargent be acquitted. But the judge's bench order and subsequent decision revealed no substantive reasoning for this reversal. So, while there may be favorable precedent to avoid tippee liability without tipper liability, where the decision provides no grounds and reveals no rationale, in the right circumstances, the SEC could continue to pursue tippee liability without tipper liability in 2024.

In addition, as we have all adjusted to a "new normal" of remote work, the SEC's focus on where to find insider trading cases has also evolved. Indeed, the SEC is aware that the changing work environment, with more individuals working from home, might make insider trading easier. In 2023, the SEC brought insider trading

charges against broker-dealer Jordan Meadow and CCO Steven Teixeira in connection with their alleged trading based on material non-public information Teixeira allegedly obtained from his girlfriend's laptop while she was working from home. According to the SEC, the scheme generated $28,600 for Meadow and $730,000 for Teixeria. This was not the only working-from-home case brought by the SEC since the pandemic. The SEC is certainly attuned to the new working-from-home environment, and we expect increased vigilance for improper trading activity occurring as a result.

Moreover, as technology continues to develop, the SEC has further honed its use of data analytics in its detection and prosecution of insider trading violations. For example, in 2023, the SEC filed four separate complaints in the Southern District of New York alleging insider trading against 13 defendants on the same day. These charges were brought in coordination with the DOJ, which likewise brought criminal charges arising from the same conduct. In remarks about these cases, the SEC acknowledged that the charges were the result of the SEC's use of data analytic initiatives and leveraging the tools at its disposal to investigate abusive trade practices: "Public trust is essential to the fair and efficient operation of our markets. But when public company insiders take advantage of their status for personal gain, as we allege here, the investing public loses confidence that the markets work fairly and for them. Today's actions reaffirm our commitment to leveraging all the tools at our disposal, including our data analytics initiatives, to investigate these abusive trading practices, hold accountable bad actors and ensure the integrity of our markets."

Finally, changes made to Rule 10b5-1 plans, which took effect in February 2023, have started to generate SEC scrutiny and enforcement actions, a trend we expect to see more of in 2024. The SEC amendments to Rule 10b5-1 update the conditions that must be met for the Rule 10b5-1 affirmative defense. Most notably, these include (1) adopting cooling-off periods before trading can commence, (2) requiring directors and officers to represent that they are not aware of any material, non-public information and that the plan is adopted in good faith, and (3) requiring continued good faith for the duration of the plan. On the heels of this rule change, the SEC brought an enforcement action against the executive chairman of Ontrak Inc. for insider trading, alleging that he sold more than $20 million of Ontrak stock while in possession of material, non-public negative information related to the company's largest customer. The chairman tried to take advantage of the Rule 10b5-1 plan he had entered into, but the SEC found he had violated Rule 10b5-1 because he was aware of material, non-public information at the time he entered into a Rule 10b5-1 plan. The SEC not only argued that the chairman could not rely on the affirmative defense under Rule 10b5-1 but also claimed the individual avoided more than $12.7 million in losses through the plan. We expect to see more cases like this in 2024 as the law continues to develop around these Rule 10b5-1 amendments.

Continued Focus on Individual Accountability

As expected, individual accountability remained a "pillar of the SEC's enforcement program" in fiscal year 2023. Similar to prior years, approximately two-thirds of the SEC's enforcement actions in the past year involved at least one individual target. These individuals ranged from company founders and executives to lower-level employees, and the alleged conduct at issue included not only traditional financial misrepresentations but also misrepresentations regarding personal behavior/misconduct (such as inappropriate workplace relationships).

For example, the SEC charged the founder of Frank, a student loan assistance company, with fraud in connection with a $175 million sale to JP Morgan Chase Bank. The SEC alleged the founder deceived JP Morgan Chase Bank by generating and misrepresenting data to appear as if Frank had 4.25 million customers when it had fewer than 300,000. Notably, the SEC did not charge the company itself, describing the founder as the "public face of Frank" and "chief negotiator" on behalf of Frank in its acquisition discussions with JP Morgan Chase Bank. In another example, the SEC charged a former Stanley Black & Decker executive for allegedly causing the company to violate proxy solicitation and receiving undisclosed compensation.

Extending its pursuit beyond founders and senior executives, the SEC also charged a bookkeeper of the Mexico-based company Aras Investment Business Group, as well as the company itself, its CEO, and three other promoters of the company. According to the SEC, defendants fraudulently raised at least $15 million from more than 450 retail investors from the Mexican-American community and promised investors monthly returns as high as 10 percent. Instead of using funds for investment purposes, defendants allegedly used funds to pay for personal expenses. The SEC also took this case as an opportunity to alert the public about affinity fraud – an investment scam that targets members of a community, such as a religious or ethnic community. Reminding investors to stay vigilant about such scams, the SEC recirculated an investor alert on how to avoid investment decisions based on common ties with someone selling an investment.

In addition to seeking monetary sanctions, the SEC also sought to hold individuals accountable in other ways. Specifically, the SEC obtained 133 orders barring individuals from serving as officers and directors of public companies, referred to as officer-and-director bars, the highest number in a decade. In one case, the SEC imposed a five-year officer-and-director bar and a $400,000 civil penalty on McDonald's former CEO after he misrepresented the circumstances leading to his termination. The former CEO allegedly failed to disclose inappropriate relationships he had with employees. The SEC alleged that he "knew or was recklessness in not knowing that his failure to disclose these . . . violations of company policy prior to his termination would influence McDonald's disclosures to investors related to his departure and compensation."

The SEC also imposed a permanent officer-and-director bar on a former Wells Fargo senior executive after she allegedly misrepresented the success of the company's core business by endorsing a metric that was inflated by unauthorized accounts. In addition to imposing a permanent bar, the SEC also imposed a $3 million civil penalty, and the senior executive agreed to pay a disgorgement of about $1.5 million.

At the 2023 Securities Enforcement Forum, Chairman Gensler stated, "Accountability includes protecting the public by barring individuals – whether from practicing before the SEC, association bars, or otherwise." As fiscal year 2024 unfolds, we expect that the SEC will continue to use bars as a corrective and deterrent tool when pursuing individual accountability.

SEC Cracks Down on Recordkeeping Requirements

In the past year, the SEC zeroed in on firms that failed to preserve employees' text messages. On August 8, 2023, the SEC found that employees at 11 firms had unapproved "off-channel" communications on their personal devices, discussing recommendations, proposals, and advice that the firm provided to investors. As a result, the firms were charged with violating recordkeeping provisions of the Securities Exchange Act and ordered to pay a combined penalty of $289 million. Just a month later, the SEC charged 10 firms for the same reason, and the firms agreed to pay combined penalties of $79 million. After self-reporting, Perella Weinberg

Partners was ordered to pay a notably lower penalty of $2.5 million, while other firms that did not self-report had to pay penalties ranging from $8 million to $35 million. On this note, Gurbir S. Grewal said, "There are real benefits to self-reporting, remediating and cooperating."

With the turn of the new year, we expect that the SEC will continue to investigate "off-channel" communications and pursue firms that fail to preserve text messages. In fact, on February 9, 2024, the SEC charged 16 additional firms for failing to preserve text messages, resulting in combined penalties of more than $81 million.

SEC Issues Final Rule Regulating SPAC Transactions

On January 24, 2024, the SEC adopted new rules and amendments strengthening the regulatory regime governing special purpose acquisition company, or "SPAC," transactions. A SPAC is a shell company with no operations created for the purpose of raising capital through an initial public offering ("IPO") and later acquiring or merging with a privately held company. In essence, SPAC transactions can be broken down into two stages: the SPAC IPO and the de-SPAC transaction, which results in an acquisition of or merger with a private company, effectively bringing that company public.

SPACs have been under intensifying scrutiny since they gained popularity in 2020. The SPAC sponsor, the entity responsible for identifying a suitable private company (commonly referred to as a target) to acquire or merge with, frequently has interests divergent from investors who purchase shares in the SPAC. Those conflicts of interest have drawn increasing scrutiny from the SEC in recent years. The new rules aim to level the regulatory playing field between traditional IPOs and SPAC transactions by enhancing disclosure requirements, holding target management accountable for their projections, and strengthening issuer obligations. Specifically, the new rules require, among other things:

- Heightened disclosure requirements at both the SPAC IPO and de-SPAC transaction stages about conflicts of interest, SPAC sponsor compensation, dilution risks amongst investors in the SPAC or the target company, and other information.
- Registrants to provide information about the types of targets the SPAC is seeking to acquire or merge with to investors at the SPAC IPO stage.
- The target company to become a "co-registrant" with the SPAC for any registration statement filed in connection with the de-SPAC transaction, such that the target company assumes responsibility for disclosures made in the SPAC's registration statement.
- Disclosures about any projections made, including disclosures related to all material bases of the projections, all material assumptions underlying the projections, and the views of the applicable board or management team regarding the projections. The rules also eliminate the safe harbor from liability for forward-looking statements in the Private Securities Litigation Reform Act of 1995 for SPACs.

The volume of de-SPAC transactions has decreased significantly since its peak in 2021, tumbling from 613 such transactions in 2021 to just 31 in 2023. Nonetheless, the new rules will make SPAC transactions subject to greater scrutiny in 2024 and beyond.

SEC Releases New Cybersecurity Disclosure Rules

On July 26, 2023, the SEC adopted final rules requiring that public companies both promptly disclose material cybersecurity incidents and provide annual reporting on their cybersecurity risk management, strategy, and governance. The rules, which we discussed last year in this webinar, are the latest in a series of efforts by the SEC to create greater uniformity and provide more rigorous guidance relating to disclosing cybersecurity risks to investors. Although the rules – which began to take effect on September 5, 2023 – create new disclosure requirements, they also leave companies with the flexibility to determine how to address cybersecurity threats based on their particular circumstances and risk profile. Companies subject to the SEC rules must now focus on creating appropriate mechanisms to provide accurate and timely information to investors.

This is not the first time the SEC has weighed in on cybersecurity risk disclosures. In 2011, SEC staff provided guidance on applying existing disclosure requirements to cybersecurity issues, and the SEC itself issued similar guidance in 2018. Despite this guidance, the SEC found that disclosure practices remained inconsistent across companies. With the rise in cybersecurity incidents and the increasing cost they are having on companies and their investors, the SEC has provided more explicit and uniform expectations through these rules.

Enforcement against misrepresentations concerning cybersecurity practices is not new to the SEC. In 2017, Enforcement created the Cyber Unit, which has been active ever since. It nevertheless remains to be seen how the SEC will approach enforcement of the new rules. While companies can take some comfort in the limited nature of the disclosure requirement – materiality, for example, is an important touchstone since only the material impacts of a material cybersecurity incident must be disclosed – the practical difficulties of investigating a cybersecurity incident, determining that it was material, and disclosing it to the SEC within the prescribed period (four business days after making that determination) is a daunting task for companies that historically may have needed a longer period of time to fully investigate and remediate an incident before disclosing.

Supreme Court Rules in Favor of Limiting the SEC's Administrative Enforcement Powers

While the Division spent fiscal year 2023 bringing enforcement actions as part of a larger trend rolling back the power of administrative agencies, the Supreme Court has taken significant steps towards curbing the SEC's enforcement powers. In *Axon Enterprise Inc. v. Fed. Trade Comm'n*, 598 U.S. 175 (2023), the Supreme Court opened the door to allow respondents in SEC enforcement actions that are presented to administrative law judges to bring collateral constitutional challenges in federal court, potentially complicating and delaying the SEC's enforcement efforts. The Court held that respondents in an SEC administrative enforcement action can bring constitutional challenges to those proceedings directly to federal district court without first raising those challenges with the Commission itself as prescribed by the Securities Exchange Act. The decision is likely to increase the number of constitutional challenges to SEC enforcement actions at the outset of those actions and provides an attractive path for litigants seeking to further challenge the Commission's power.

The Supreme Court also appears poised to restrict the SEC's enforcement power by barring its ability to bring enforcement actions based on securities fraud before administrative law judges (ALJs). In *SEC v. Jarkesy*, a case currently pending before the Supreme Court, a Texas-based hedge fund manager challenged the SEC's enforcement action against him on constitutional grounds. An ALJ found that Jarkesy committed securities fraud when he made misrepresentations about his funds to investors. The Commission imposed a penalty, required Jarkesy to disgorge profits, and barred him from investment-related activities. The Fifth Circuit

vacated the decision in a sweeping opinion, holding that: (1) the use of ALJs violates the Seventh Amendment right to a jury trial; (2) Congress impermissibly delegated legislative power by allowing the Commission to decide whether to bring enforcement actions before AJLs or in federal court; and (3) the protection against removal of ALJs were unconstitutional. In November 2023, the Supreme Court heard oral arguments and largely focused on the issue of whether the SEC's use of ALJs violated the Seventh Amendment. The six conservative justices expressed concerns about agencies' use of ALJs and the increasing scope and power of the administrative state. If the Supreme Court affirms the Fifth Circuit's decision on the Seventh Amendment issue, the SEC will no longer be able to bring enforcement actions in cases of securities fraud before ALJs, depriving them of a critical enforcement tool. The decision would force the SEC to bring such claims in federal courts, which would provide defendants with access to a jury trial and protections under the Federal Rules of Civil Procedure and Evidence. We expect a decision from the Supreme Court by June 2024.

REFLECTING ON HIGHER EDUCATION COMPLIANCE AND INVESTIGATIONS TRENDS IN 2023 AND LOOKING AHEAD TO 2024

by Madeleine K. Rodriguez, Anthony D. Mirenda and Susanna Chi

2023 was a contentious year for higher education institutions. Whistleblowers, activists and other interested third parties doggedly pursued alleged research misconduct affecting renowned scholars and consequential studies. The federal government continued its use of sanctions and export controls as foreign policy tools, increasing the compliance complexity for research universities. Colleges were caught in the crosshairs of political activism regarding Israel and Palestine, called to defend their commitment to free speech and academic freedom while balancing the responsibility to maintain school environments free from antisemitism and Islamophobia, resulting in investigations from all sides. And several major universities confronted antitrust allegations, challenging some schools' financial aid practices.

As they tackled a slew of challenges on multiple fronts, all the while facing the national spotlight, higher education and research institutions faced the overarching, and perhaps existential, quest to regain trust among diverse groups in our society.

Against this backdrop, we take a moment to assess major issues impacting colleges, universities, and other leading research institutions. We also look ahead, anticipating the next wave of challenges in 2024.

Research Misconduct Will Remain Under a Microscope

In 2023, allegations of data manipulation and plagiarism reverberated throughout academic communities across the country and, at times, made headlines that extended beyond research campuses and into broader society. We first highlight some cases regarding data manipulation, followed by a discussion of a growing trend in the use of AI to detect potential plagiarism.

Whistleblowers, activists and other interested parties continue to raise claims of data manipulation, plagiarism or other research misconduct.

This past year saw a wide variety of cases alleging data manipulation. The allegations cut across a variety of research topics, ranging from an experimental drug for stroke patients to a behavioral economics study on honesty. The parties raising the allegations also varied widely and included not only peers within the same academic community, but also former lab members, so-called "watchdog" blog sites, and an undergraduate student journalist. Because such research is often inextricably intertwined with government grants or private funding that ties back to the potential commercialization of highly valuable products (e.g., cutting-edge drugs), bounties under the federal False Claims Act and stock market profiteering provide considerable financial incentives to surface allegations of misconduct.

For example, Berislav Zlokovic, University of Southern California ("USC") Chair and Professor of Physiology and Neuroscience, faced scrutiny after a group of whistleblowers, including Matthew Schrag, a Vanderbilt assistant professor and Elisabeth Bik, a Dutch microbiologist, alleged Zlokovic used fraudulent data to promote an experimental drug developed to limit brain damage after strokes.

Schrag and Bik submitted a 113-page dossier to the National Institutes of Health ("NIH") that pointed to evidence of alleged image manipulation, where some cells were supposedly erased, and nuclei of others were obscured. Former members of Zlokovic's lab also reported a culture of professional intimidation, claiming Zlokovic instructed his team to alter entries in lab notebooks.

In response, on November 16, 2023, NIH launched an investigation and paused the start of a $30 million trial for the experimental drug. USC also opened an internal investigation into Zlokovic. Because federal grant funds are allegedly involved, it is reported that some of the whistleblowers may file a federal False Claims Act lawsuit that could give them a portion of NIH funds that the government claws back if Zlokovic's work is proven to be the product of fraud.

In another case, the blog Data Colada raised questions regarding the research of Duke Professor of Psychology and Behavioral Economics Dan Ariely. In 2021, Ariely and his co-researchers released a study suggesting that people were less likely to lie on a form if they signed an honesty pledge at the top rather than the bottom. After other researchers reported they were unable to replicate the study, Data Colada investigated the study's data and claimed it found certain anomalies, such as suspiciously "uniform" data points.

In response, Duke conducted a full investigation, increased its oversight of Ariely's Center for Advanced Hindsight, and required Ariely to participate in an eight-week course on professionalism and integrity.

In one of the most high-profile cases, an eighteen-year-old student journalist published allegations of research misconduct against Stanford University President Marc Tessier-Lavigne. A university investigation found an "unusual frequency of manipulation of research data and/or substandard scientific practices" by junior researchers in Tessier-Lavigne's labs and concluded that Tessier-Lavigne "failed to decisively and forthrightly correct mistakes in the scientific record," though the investigation also found that Tessier-Lavigne himself had not engaged in research misconduct. Following these allegations and investigation, Tessier-Lavigne stepped down as president of Stanford.

As a result of these investigations and others in the past year, federal funding agencies are viewing research studies past, present, and future with increased skepticism and heightened scrutiny. As 2024 makes its way, we expect a rising probe into academic research across all disciplines from federal agencies and whistleblowers from all backgrounds and an increased appetite to ferret out potential data manipulation.

AI is increasingly used to identify potential plagiarism.

The past year also surfaced a notable trend relating to AI that we foresee influencing how individuals attempt to detect potential plagiarism in 2024.

For example, Bik, an image forensics specialist and one of the researchers who raised concerns with Zlokovic's work, reportedly uses an AI-based software called ImageTwin, which is said to scan images in a paper and then compare them with other images. The ubiquitous nature of these types of technologies will undoubtedly lead to more allegations and the need for more investigations.

Research Institutions Likely to Confront Complex Cross-Border Compliance Issues

Cross-border compliance issues continue to increase in complexity and scope. Russia's invasion of Ukraine moves into its third year, Iran continues to assist Russia's war effort and support U.S.-designated terrorist organizations in the Middle East, and national security and economic issues with China grow ever more complex. As the U.S. and other Western nations expand their efforts to use sanctions and export controls as foreign policy tools, the compliance landscape involving Russia, China, and Iran (as well as other countries) continues to evolve dramatically, increasing the compliance complexity for research universities and other higher education institutions.

In addition, early in 2023, the federal government launched the Disruptive Technology Strike Force as a way of reinvigorating investigation and compliance efforts in the wake of the discredited "China Initiative." The Strike Force represents a collaboration between the Department of Justice and the Department of Commerce, who describe the initiative as part of a "whole-of-government approach" to targeting illicit actors, strengthening supply chains, and protecting critical technologies from being acquired or used by nation-state adversaries such as China, Russia, Iran, and North Korea. One of the Strike Force's stated goals is to foster partnerships with the private sector in protecting U.S. advanced technologies from illegal acquisition and use by nation-state adversaries. The Strike Force is focused on technologies that could advance military capabilities or mass surveillance programs that enable human rights abuses, including, for example, those related to supercomputing and exascale computing, artificial intelligence, advanced manufacturing equipment and materials, quantum computing, and biosciences. We expect Strike Forces around the country to continue to reach out to a wide range of private sector actors, including research universities and labs, to gain a better understanding of the landscape and to target enforcement activities more effectively.

Colleges Will Continue to Face Tensions Among Title VI, Free Speech, and Academic Freedom Claims

The ongoing Israel-Palestine conflict presents uniquely challenging enforcement issues for universities. Contrasted with other moments of increased activism and student or faculty-led protests on campus, both groups here are protected classes entitled to Title VI's guarantees of an educational environment free from discrimination and harassment. Higher education institutions have an obligation to ensure that students are not subject to disparate treatment or a hostile environment based on their real or perceived identities as Jewish, Muslim, Israeli, Palestinian, or Arab, all the while balancing an increased focus on academic freedom and the importance of free speech rights on campus. The result is an environment that can often feel almost impossible to navigate without the institution being on the receiving end of a complaint, lawsuit, or reputational scrutiny.

Department of Education's Office for Civil Rights expected to continue seeing an increase in Title VI complaints.

In the months since Hamas' attack on Israel on October 7, 2023, and the ongoing war in Gaza, the Department of Education's Office for Civil Rights ("OCR") has received a downpour of Title VI complaints related to the law's protections for students based on real or perceived shared ancestry or ethnic characteristics. The

Department of Education is investigating more than three dozen colleges regarding complaints that the institutions allegedly failed to properly address instances of antisemitism or Islamophobia.

In response to the surge in Title VI complaints and general reports of bias-motivated incidents on campuses, OCR released a Dear Colleague Letter on November 7, 2023. In this Dear Colleague Letter, OCR expressed an "alarming rise in disturbing antisemitic incidents and threats to Jewish, Israeli, Muslim, Arab, and Palestinian students on college campuses" and reminded education institutions of their "legal responsibility under Title VI of the Civil Rights Act of 1964 . . . to provide all students a school environment free from discrimination based on race, color, or national origin, including shared ancestry or ethnic characteristics."

There are no signs that tensions on campuses will quell in 2024. In fact, on January 22, 2024, advocacy groups Louis D. Brandeis Center for Human Rights Under Law and Jewish on Campus filed a complaint with OCR against American University. Alleging Title VI violations, the complaint contains witness statements from twelve anonymous American University students who were allegedly "threatened, marginalized, shunned, and made to feel unwelcome in their dormitories, classrooms, and social spaces throughout the campus."

Just seven days later, another advocacy group filed a complaint with OCR. This time, the Muslim Legal Fund of America ("MLFA") filed a complaint with OCR on behalf of a dozen Harvard students. MLFA's complaint demanded an immediate investigation into Harvard's alleged failure to protect these students from harassment, intimidation, and threats based on their identities as Palestinian, Arab, Muslim, and supporters of Palestinian rights.

Students are raising Title VI claims in court.

In addition to filing complaints with OCR, students are suing universities in federal courts. For example, two current students sued the University of Pennsylvania on December 5, 2023, under Title VI for allegedly "subject[ing] [Jewish students] to a pervasively hostile educational environment" and "plac[ing] plaintiffs and other Jewish and Israeli students at severe emotional and physical risk." In November 2023, students also sued the University of California Berkeley and New York University for alleged violations of Title VI based on antisemitism following the October 7 attack. A former student sued Carnegie Mellon University under Title VI on December 13, 2023, based on antisemitism, although her factual allegations do not stem from the October 7 attack.

Students are defending their First Amendment right to advocate on campuses.

In one very high-profile case, a pro-Palestine student group filed for declaratory and injunctive relief against Florida Governor Ron DeSantis and other state officials, including the Chancellor of the State University System of Florida, Raymond Rodrigues, and members of the Florida Board of Governors of the State University System. *See Students for Justice in Palestine at the University of Florida v. Rodrigues et al.*, 1:23-cv-00275. According to the complaint, Rodrigues released a memorandum, in consultation with DeSantis, calling on colleges in Florida's state university system to "deactivate" their Students for Justice in Palestine chapters.

Raising a First Amendment challenge, the pro-Palestine student group argued that Rodrigues' memorandum violates the First Amendment's protections against viewpoint-based restrictions on speech and association. The student group also argued that Rodrigues' charge to "deactivate" pro-Palestine student groups stifles

"pro-Palestinian advocacy on campus at a time when the Palestine-Israel conflict is a matter of vital public discourse and concern."

Just last month, the Florida court denied the request for preliminary injunction, finding that the student group lacked standing because it failed to demonstrate a substantial likelihood of establishing an injury-in-fact. The court based this decision on the determination that neither DeSantis, Rodrigues, nor the Board of Governors have the authority to punish student organizations. Instead, the Boards of Trustees of its constituent universities have such authority, but the record lacked any evidence that the Boards of Trustees had taken any steps to "deactivate" the student group. In February, the Court dismissed the complaint against all defendants.

Professors are raising concerns about academic freedom.
Adding to rising tensions on campus, professors have also raised academic freedom challenges, surfacing concerns about colleges' restrictions on political speech. For example, the Department of Women's, Gender and Sexuality Studies at Barnard College posted a statement on its departmental website titled "Solidarity with Palestine." Two days later, Barnard administrators removed the statement from the departmental website and subsequently updated the College's political activity policy. In response, the New York Civil Liberties Union ("NYCLU") sent a letter to Barnard College President Laura Rosenbury, raising free speech and academic freedom concerns. While faculty members, with the help of the NYCLU, are working with the College to see if it is possible to republish a similar statement on the College's website that comports with the new political activity policy, it remains to be seen whether a compromise can be reached, and if so, whether other interested parties will raise challenges to any statement that results from such a resolution.

As the Israel-Palestine conflict continues and devastation, fears, and anxieties continue to mount, colleges will have to be particularly careful and nimble about ensuring all members of their community experience not only an environment free from discrimination and harassment but also an environment that maintains and safeguards spirited dialogue for all viewpoints represented within their community.

But what about Students for Fair Admissions?
In one of the most monumental cases from the past year, the Supreme Court held in *SFFA v. Harvard College* and *SFFA v. University of North Carolina* that Harvard and University of North Carolina's admission policies violated the Equal Protection Clause of the Fourteenth Amendment (in UNC's case) and Title VI (in Harvard's case). Zeroing in on Justice Gorsuch's concurrent opinion, where he drew the connection between Title VI and Title VII, opponents of affirmative action began immediately challenging diversity, equity, and inclusion ("DEI") policies in the employment context. For example, Attorney Generals of thirteen states issued a cease-and-desist letter to Fortune 100 CEOs, alleging "racial discrimination is commonplace among Fortune 100 companies and others," and advocacy group America First Legal filed dozens of letters with the Equal Employment Opportunity Commission, alleging that companies are implementing discriminatory DEI policies in violation of Title VII.

While the immediate aftermath of *SFFA* has largely focused on corporate America's DEI programs, we expect the focus will return to higher education institutions, especially once the results of the first post-*SFFA* admissions cycle are released.

Universities will also have to brace for discrimination claims that extend beyond admissions practices, as litigants are poised to launch claims against universities with programs and scholarships for underrepresented and disadvantaged students. For example, in November 2023, another advocacy group known as the Equal Protection Project ("EPP") filed a complaint against the University of Colorado ("CU") in Boulder and Denver with OCR. Specifically, EPP alleges that CU-Boulder and CU-Denver violate the Equal Protection Clause and Title VI by participating in the McNair Scholarship Program, a federal program for students from underrepresented groups. More complaints like EPP's are expected to come in 2024.

Other universities may face increased pressure to settle in antitrust lawsuits.
In 2022, former students filed an antitrust lawsuit against seventeen private universities (the "Universities"). *See Henry et al. v. Brown University et al.*, 1:22-cv-125. Plaintiffs claimed that the Universities purportedly colluded on financial aid awards by allegedly sharing confidential data about financial aid and admissions and agreeing on a methodology to determine students' financial aid. Plaintiffs further claimed that, as a result of the alleged conduct, Universities reduced the amount of financial aid to about 200,000 financial aid recipients and "artificially inflated the net price of attendance for students receiving financial aid."

Plaintiffs claimed that the Universities were not entitled to an antitrust exemption because this exemption applies to agreements between universities in which all students are admitted on a need-blind basis. According to plaintiffs' claims, the Universities considered prospective students' financial circumstances when deciding whether to admit students.

Plaintiffs sought compensation for themselves and a class of U.S. citizens or permanent residents who enrolled in the Universities' full-time undergraduate programs, received need-based financial aid, paid for tuition, room, and board not fully covered by financial aid, and first enrolled in one of the Universities' full-time undergraduate programs at the time the Universities respectively implemented the purported agreed-upon methodology. Plaintiffs alleged most of the Universities implemented the methodology in 2003, while other Universities allegedly implemented it later, in 2004, 2019, and 2021, respectively. The class also included parents, legal guardians, and other family members who paid the Universities on behalf of students.

On July 7, 2022, the Antitrust Division of the Department of Justice ("DOJ") filed a Statement of Interest, contending that plaintiffs "adequately alleged" that the Universities' purported agreement on a common methodology violated the Sherman Act. The DOJ also contended that the Universities' argument that the antitrust exemption protects those who lack actual knowledge that other member schools are not need-blind "stretches" the exemption "beyond its extent" and "superimposes an intent requirement on the application of the [e]xemption." About a month later, the Court denied the Universities' motion to dismiss.

Since then, settlement agreement negotiations have been underway. On April 19, 2023, the University of Chicago was the first to announce its decision to settle and agreed to pay $13.5 million to class members. As part of the settlement agreement, the University of Chicago agreed to cooperate with plaintiffs on certain discovery matters by providing documents and facilitating witness interviews which may help plaintiffs' case against other Universities.

At the start of the new year, several other universities followed suit, with Brown, Columbia, Duke, Emory, and Yale agreeing to a combined settlement payment of $104.5 million. On February 23, 2024, Dartmouth, Northwestern, Rice, and Vanderbilt reached settlements totaling $166 million. With seven Universities remaining in the lawsuit, we expect more settlement negotiations as the year progresses.

As we wait for more potential settlements, we take a moment to recognize the lesson that this antitrust case teaches: While the nature of higher education is inherently collegial, there is a limit to the level of collaborative decision-making and coalition-building that is permissible among universities without running afoul of antitrust laws. Moving forward, schools should take care to ensure they are not improperly overextending their collaboration and coordination. This applies not only to issues like financial aid and admissions practices but also potentially to other issues, including athletics, hiring, and institutional policies and practices.

ANTICORRUPTION ENFORCEMENT AND THE FOREIGN CORRUPT PRACTICES ACT: TRENDS TO TRACK IN 2024

by Anthony D. Mirenda, Shrutih Tewarie and Jack C. Smith

The past year was an active one for developments in anticorruption enforcement, particularly in the U.S., featuring multiple significant policy pronouncements, a brand new anti-bribery enforcement statute, plenty of corporate and individual Foreign Corrupt Practices Act (FCPA) enforcement activity, and cross-border collaboration with multinational law enforcement partners. Below, we review the key moments from 2023 and plot out the trends to watch in 2024.

U.S. POLICY DEVELOPMENTS

The Biden Administration's Anti-Corruption Strategy

On December 11, 2023, the Biden administration issued a statement on "U.S. Leadership in the Fight Against Global Corruption," ("2023 Leadership Statement") reiterating the administration's position that "countering corruption [i]s a core U.S. national security interest." This follows the 2021 "U.S. Strategy on Countering Corruption" ("2021 Anti-Corruption Strategy"), the first such articulation of an anti-corruption strategy issued by a president. The 2023 Leadership Statement provided progress updates on the five pillars of the 2021 Anti-Corruption Strategy:

1. Modernizing, Coordinating, and Resourcing U.S. Efforts to Fight Corruption
2. Curbing Illicit Finance
3. Holding Corrupt Actors Accountable
4. Preserving and Strengthening the Multilateral Anti-Corruption Architecture
5. Improving Diplomatic Engagement and Leveraging Foreign Assistance

Alongside the 2023 Leadership Statement, President Biden issued a Presidential Proclamation restricting entry to the U.S. for non-U.S.-residents who enable corruption. While earlier proclamations from prior administrations had covered similar ground, this proclamation purports to fill a gap in the prior orders and symbolically demonstrates anti-corruption among the administration's priorities. The 2023 Leadership Statement portends further executive action stemming from this proclamation, specifically the "use [of] existing sanction authorities to target private enablers of public corruption – including by freezing their assets."

Foreign Extortion Prevention Act: New Law Targets Demand-Side of Foreign Corruption

As we have previously analyzed in greater detail here, on December 22, 2023, President Biden signed into law the Foreign Extortion Prevention Act ("FEPA"). FEPA imposes direct criminal liability on foreign officials who demand, seek, receive, or accept bribes from U.S. companies or individuals or any person while in the territory

of the United States. By targeting the demand side of bribery, FEPA serves as a complement to the FCPA, which targets the supply side by prosecuting individuals and companies that pay bribes to foreign officials.

While the Department of Justice has, in some cases, prosecuted foreign government officials who obtained bribes under other legal theories, including particularly the money laundering statute (18 U.S.C. § 1956), FEPA provides the government with another potentially powerful tool for these enforcement actions. Nonetheless, the sensitivities and political difficulties with prosecuting foreign government officials still exist, regardless of the statutory offense, so it remains to be seen whether FEPA will substantially increase actions against foreign government actors. Acting AAG Nicole Argentieri recently pointed to these sensitivities in public remarks announcing that, as is the case for the FCPA, FEPA cases will be run centrally out of the Department's Fraud Section rather than out of individual U.S. Attorney's Offices.

Observed Trends from Corporate Enforcement Policy (CEP) Revisions

As we previously covered, DOJ in January 2023 announced revisions to the Corporate Enforcement Policy seeking to clarify the benefits offered for self-disclosure of misconduct and revising the credits available for cooperation. Through subsequent remarks from Acting AAG Argentieri in November 2023 and March 2024, DOJ has highlighted several key trends from actions implementing the CEP revisions.

First, Acting AAG Argentieri highlighted that corporate resolutions and declinations have directly led to charges against individuals–reinforcing that cooperation by companies, in DOJ's view, often means identifying – and thereby facilitating the prosecution of – culpable individuals. Second, the revised CEP is increasingly bearing fruit: In 2023, DOJ received nearly twice as many voluntary disclosures as in 2021. Third, even for those companies that *did not* self-disclose, the newly-raised 50% cap on cooperation and remediation credit available to such companies has already been borne out in resolutions with Albermarle Corporation (45% reduction) and SAP SE (40% reduction).

Pilot Program Regarding Compensation Incentives and Clawbacks

On March 3, 2023, DOJ announced a new Pilot Program Regarding Compensation Incentives and Clawbacks to run for three years in this pilot form. Under this two-part program, DOJ will require, as part of a criminal resolution, that corporate compliance programs include compensation-related criteria, and it will also offer fine reductions for companies that seek to claw back compensation from culpable employees in appropriate cases. The pilot program has already resulted in additional credit for SAP in a resolution announced in January 2024. DOJ highlighted that even before the resolution, SAP had already modified its compensation incentives to accord with compliance goals; SAP then also committed to further incorporating compliance into compensation and bonus systems, as required under the program. Under the second prong of the program, DOJ credited SAP with $109,141 against its fine amount for compensation the company withheld from employees (though this amount is relatively small compared with the overall $221 million resolution) and also credited the company's efforts to defend these clawbacks in litigation as part of the company's overall cooperation efforts, which resulted in a 40% total fine reduction.

Safe Harbor for Self-Disclosures in Connection with Mergers and Acquisitions

As we previously discussed, in October 2023, Deputy Attorney General Lisa Monaco announced a new safe harbor policy that grants presumptive declinations to acquiring companies that self-disclose criminal misconduct in an acquired company within six months of the merger transaction (the "Safe Harbor period")

and otherwise cooperates and remediates the misconduct. In March 2024, this policy was codified in a new provision of the Justice Manual. One recent FCPA declination issued to Lifecore Biomedical, Inc. demonstrated the potential implications of the safe harbor, though the new policy was not expressly cited in the declination. Lifecore acquired Yucatan Foods L.P. in 2018, and, in part because at least one Yucatan officer actively concealed the bribery misconduct during pre-acquisition diligence, Lifecore did not learn of it until a post-acquisition internal investigation. The declination letter noted the speed of Lifecore's voluntary self-disclosure: within three months of discovering the possibility of misconduct and "hours" after their investigation confirmed it.

New DOJ Whistleblower Reward Pilot Program

In remarks delivered on March 7, 2024, Deputy AG Lisa Monaco announced that the Department would commence a new whistleblower reward program, initially as a pilot program, and Acting AAG Nicole Argentieri then announced on the following day the Department's intent to apply the policy specifically in the FCPA context. According to Acting AAG Argentieri, "[W]e anticipate that the program could prove especially useful in developing foreign corruption cases that are outside the jurisdiction of the SEC, including FCPA violations by non-issuers."

Under the proposed initiative, whistleblowers who provide "original, nonpublic, truthful information" about corporate wrongdoing not otherwise known to the government may be eligible to receive a portion of any restitution, provided an investigation results in a substantial penalty above a to-be-determined threshold amount.

Opinion Procedure Releases

Last year, we noted the rarity of DOJ issuing opinion procedure releases (OPRs) in recent years, with a 2022 release only the second since 2014. Last year, the Department issued two OPRs, in August and October 2023. The uptick represents a small but positive trend in the Department's willingness to provide actionable guidance outside of an enforcement action or broadly prepared remarks. Moreover, each OPR was released within two months of the initial request and one month of the submission of supplemental information, reflecting shorter response times than had historically been seen.

The August release concerned a U.S.-based adoption agency seeking clarity on whether it could pay for the travel of officials from a foreign government's adoption authority to assess the success of recent adoption placements in the U.S. As with prior releases concerning adoption agencies, the Department indicated that payment for reasonable travel expenses for the legitimate visit of these officials would not be a violation due to the absence of corrupt intent for "bona fide" expenses.

The October release was requested by a company that had been awarded a task order as part of a contract with a U.S. agency to provide logistical support services, including meal and travel stipends, to foreign government personnel. DOJ determined that providing the proposed stipends would not represent an FCPA violation because the requestor lacked corrupt intent, as evidenced by the requestor's belief that the stipends had been authorized by the Foreign Assistance Act, were called for by a U.S. government program, and would be paid through a U.S. government official intermediary.

U.S. Caselaw Developments

In a much-awaited ruling, the U.S. Court of Appeals for the Fifth Circuit declined to join the Second Circuit in rejecting the application of conspiracy or aiding and abetting liability to foreign nonissuers not otherwise covered by the Foreign Corrupt Practices Act. *United States v. Bleuler*, 60 F.4th 982 (5th Cir. 2023). The *Bleuler* opinion is noteworthy in the sparsely litigated FCPA landscape for the willingness of a federal court of appeals to decline to adopt the narrow Second Circuit view of FCPA secondary liability. In *Bleuler*, the Fifth Circuit reversed the district court's dismissal of an FCPA indictment, finding that it sufficiently alleged direct violations by enumerated actors (as two agents of a domestic concern and one person acting on U.S. soil). The court turned to the government's alternative argument that the defendants were secondarily liable for conspiring with enumerated actors, and, while finding it unnecessary to reach this theory, the court expressly stated that it "neither accepts nor rejects the theory that an individual who falls outside of the actors enumerated in the FCPA can be held liable as a conspirator under a secondary-liability theory." 60 F.4th at 996 n.6.

As we have written extensively about here and here, the Second Circuit in 2018's *United States v. Hoskins* decision held that conspiracy liability cannot be used to prosecute under the FCPA any actors other than those specifically enumerated in the statute (i.e., domestic concerns, any person acting on U.S. soil, and U.S. issuers). 902 F.3d 69, 72-73 (2d Cir. 2018).

Had the Fifth Circuit directly addressed the secondary liability issue, it would have been the first appellate court to disagree with the Second Circuit, but not the first court overall. In 2019's *United States v. Firtash*, 392 F. Supp. 3d 872 (N.D. Ill. 2019), a district court in the Northern District of Illinois even more expressly rejected the position that foreign nationals can only be charged with FCPA violations if they are among the statute's enumerated actors. The issue thus appears ripe for a circuit split but will have to await the emergence of another case vehicle.

FCPA ENFORCEMENT TRENDS

A review of DOJ's Fraud Section Year in Review reports reveals that the number of corporate actions resolved has been relatively stable over the past three years but is still down significantly from the elevated numbers seen from 2016-2020. Total dollars in sanctions imposed in 2023 were down significantly from 2022, though that mark was heavily skewed by the $701 million Glencore resolution, which by itself represented more than all resolutions in 2023 ($657 million). Nonetheless, total sanctions in 2023 were down more than 90% from 2020. Notably, individual prosecutions—both in charges and in convictions—declined significantly in 2023, continuing a downward trend from the past three years.

Below, we examine some of the major FCPA enforcement actions of the past year to identify noteworthy themes and trends for practitioners to watch in 2024.

Key Individual Prosecutions

Despite the downward trend in prosecution numbers, DOJ continues to place paramount significance on the prosecution of individuals, uniformly highlighting such actions in public remarks throughout the year and noting their significance when discussing declinations and corporate resolutions. As Acting AAG Argentieri recently stated, "Our first priority has been — and will continue to be — individual accountability. Companies can only act through individuals."

First, following a long trend, the wide-ranging Petrobras investigation continues to yield enforcement actions, with a U.S.-based oil and gas trader, Glenn Oztemel, indicted for his alleged role in the scheme to pay bribes to Brazilian officials to win contracts with the state-owned entity Petrobras.

Second, in February 2024, after an eight-week trial in the Eastern District of New York, Javier Aguilar, a former executive and oil trader with Vitol Inc., was convicted of FCPA and money laundering charges in connection with a purported scheme to bribe officials in Ecuador and Mexico to obtain contracts from Petroecuador and Petróleos Mexicanos (aka "Pemex"). Vitol previously resolved a corporate action arising from the same allegations, agreeing to pay $163 million in 2020 as part of a DPA. Aguilar's case was notable in particular for the court's mid-trial ruling that employees of a unit of Pemex, Pemex Procurement International (PPI), were not "public servants" under Mexican law, and thus the particular Mexican bribery law could not serve as a predicate specified unlawful activity (SUA) for the money laundering charges. Aguilar then argued that if payments to PPI officials did not violate Mexico's bribery law, then they were legal under the FCPA's affirmative "local law" defense, which excuses conduct where the "payment, gift, offer, or promise of anything of value that was made, was lawful under the written laws and regulations of the" foreign country. 15 U.S.C. 78dd-2(c)(1). In another mid-trial ruling, however, the court rejected Aguilar's premise that conduct that did not violate Mexico's bribery law would necessarily be legal under local law and, therefore, declined to instruct the jury on this defense.

Corporate Resolution Trends

DOJ stringently parses the timeliness of voluntary self-disclosures and cooperation

Several contrasting corporate resolutions demonstrated the scrutiny with which DOJ considers the timeliness of voluntary self-disclosure and cooperation.

Consider the resolution with Albemarle, which received under the new Corporate Enforcement Policy (CEP) a 45% reduction for extensive cooperation and timely remediation—i.e., before DOJ involvement. Albemarle withheld bonuses from culpable individuals and started revamping its compliance program immediately. Acting AAG Argentieri highlighted this as a positive example of the speed of the company's remediation and cooperation, as contrasted with a more "reactive" entity in Tyser Insurance Brokers, which received only a 25% reduction.

And yet, despite being elevated in public remarks as a "timely" cooperator who had self-disclosed, Albemarle still did not receive the maximum credit possible, which it could have received under the Voluntary Self-Disclosure (VSD) component of the CEP. VSD, combined with cooperation and remediation, can make a company eligible for a reduction of up to 75%. But DOJ declined to award full VSD credit to Albemarle because, in DOJ's view, its disclosure was not "reasonably prompt."

While the Albemarle resolution may leave open questions about DOJ's view of "reasonably prompt" disclosure, at least one company clearly met that mark. In its declination letter to Lifecore, as discussed above, DOJ credited the company's "report[ing] to the Criminal Division, Fraud Section's FCPA Unit within *three months of first discovering* the possibility of misconduct and *hours* after an internal investigation confirmed that misconduct had occurred."

Finally, at the extreme opposite end of the spectrum of timeliness of disclosure, DOJ announced a further resolution with Telefonaktiebolaget LM Ericsson ("Ericsson") in light of breaches of its 2019 Deferred Prosecution Agreement (DPA). Ericsson pleaded guilty and paid a criminal penalty of more than $206 million after admitting the breaches (this was in addition to the more than $520 million that it had paid in connection with the 2019 DPA). The breaching conduct included failure to fully disclose to the government facts and evidence related to bribe schemes in Djibouti and China, as well as conduct in Iraq representing further potential FCPA violations beyond that contemplated in the 2019 DPA.

As described in materials submitted to the court, the Djibouti evidence withheld from the government included a particular incriminating email from 2011 that had not been disclosed to the government but which had been part of an email thread whose other iterations had been produced, and the incriminating email would have been responsive to agreed-upon search terms had those terms been run in the email's language (Italian), which was a language known to Ericsson to be used by the key employee subjects of the investigation. The China evidence withheld included a key internal 2018 email making serious allegations that the company then investigated independently for three years before disclosing to the government—long after entering the DPA. The company also maintained certain records concerning third-party agreements and payments—including those relating to the China conduct—in hard copy files and USB drives at its headquarters in Sweden but failed to disclose the existence of these records until 2021.

Finally, the company's prior counsel had disclosed the beginning of an investigation into conduct in Iraq days before entering the 2019 DPA but did not include material findings then known to the company, which did not then update the government on its findings until prompted by a 2022 news report inquiry.

Acting AAG Argentieri later commented on the breach by noting that the disclosure lapses "prejudice[ed] the government's ability to charge certain individuals," such that Ericsson's additional penalties included the rescission of all cooperation credit originally granted. The cautionary tale of the Ericsson saga demonstrates in stark terms that once a company does decide to disclose misconduct and cooperate, it must do so *completely* or risk additional sanctions and losing any benefit of its cooperation.

Assisting with individual prosecutions facilitates declinations and cooperation credit

Consistent with DOJ's repeated emphasis on the importance of individual prosecutions, several actions this year illustrated how facilitating individual prosecutions played into corporate declinations and cooperation credit.

First, Acting AAG Argentieri highlighted the role of individual prosecutions in the Corsa Coal Corporation resolution. As part of its extensive cooperation, the company provided evidence about individual wrongdoers, including two former vice presidents who were charged criminally for their involvement in the scheme. Argentieri noted "This is a perfect example of our policies in action: offering appropriate incentives for a company to do the right thing and tell us about a scheme we were not aware of, resulting in criminal charges against culpable executives."

U.K. Insurance brokers H.W. Wood Ltd. and Tysers Insurance Brokers Ltd. further illustrated this principle. A 2022 FCPA voluntary self-disclosure from another company, Jardine Lloyd Thompson Group Holdings Ltd., led to the prosecution of four individuals connected to that company as well as information about other corporate

actors H.W. Wood and Tysers (formerly Integro) involved in similar misconduct. Jardine Lloyd Thompson then received a full declination, compared to the less favorable outcome for Tysers, which entered a DPA and received a relatively lesser 25% credit off its fine due to remedial measures taken by the company. In the announcement of the resolutions with H.W. Wood and Tysers, DOJ highlighted that these investigations had now led to charges against eight individuals.

Recidivism factors substantially into DOJ enforcement decisions

As a stated factor in the Corporate Enforcement Policy, recidivism plays a prominent role in resolutions, but DOJ's discussion of recidivism in recent actions reveals that not all prior enforcement actions are treated alike. Specifically, the Department has contrasted the recidivism of two companies that entered resolutions in 2023 and 2024: Gunvor S.A. and SAP. SAP received a relatively high 40% reduction in penalty for its resolution of bribery allegations concerning South African and Indonesian officials, even with prior resolutions (i.e., recidivism) taken into account. SAP had engaged in, by DOJ's estimation, "significant prior misconduct" concerning export controls and, five years earlier, FCPA violations in Panama. Nonetheless, DOJ noted—apparently to explain the treatment of the prior FCPA offense—that SAP conducts business all over the world and has many "touchpoints" with various regulators internationally.

By contrast, Gunvor received a 25% reduction in the applicable fine in connection with a scheme to bribe government officials in Ecuador, and this was taken from the 30th percentile above the bottom of the guidelines, representing significantly less favorable treatment. DOJ emphasized that this treatment stemmed largely from the fact the Ecuadorian-official bribery took place while Gunvor was under investigation by Swiss authorities for a separate scheme to bribe officials in Africa (resolved with Swiss authorities in 2019, as part of which Gunvor admitted having inadequate anti-bribery controls). But DOJ did not explain why Gunvor was not credited for its global business model and "touchpoints" with regulators in the same way that SAP was.

The contrasts may leave practitioners with more questions than answers about the treatment of a company's prior conduct, but it appears at the least that arguments remain available for distinguishing past conduct and negotiating its impact on cooperation and remediation credit.

ANTI-CORRUPTION DEVELOPMENTS ON THE GLOBAL STAGE

U.S. Continues to Promote Collaboration with International Enforcement Agencies

Several events from 2023 highlighted the growing role of the U.S. in driving collaboration with other nations' enforcement agencies.

In August 2023, DOJ announced that Corporación Financiera Colombiana S.A. ("Corficolombiana"), a Columbian financial services institution, had agreed to criminal and civil resolution with U.S. and Colombian authorities to resolve FCPA charges. The Department touted this resolution as the first joint resolution between the two countries. This action involved a conspiracy with Brazilian construction conglomerate Odebrecht S.A., which had itself been the subject of a record $3.5 billion FCPA resolution in 2016. That earlier case required extensive collaboration with Brazilian and Swiss authorities, and the Corficolombiana resolution demonstrates an expansion of such collaboration to Colombian authorities. Moreover, DOJ credited the company for penalties paid to the Colombian authorities in the same way it had credited Odebrecht for making such payments to Brazilian and Swiss authorities.

Finally, perhaps as a logical extension of these successful cross-national collaborative efforts, Acting AAG Argentieri announced a new DOJ resource specifically designed to enhance such efforts: the International Corporate Anti-Bribery Initiative (ICAB). ICAB will task three U.S. prosecutors to specific global regions to work with local counterparts, whose mission will be to share information and develop foreign bribery cases with their local agencies.

U.K. Developments

The U.K. Serious Fraud Office (SFO) appointed a new Director, Nick Ephgrave, following the conclusion of the five-year tenure of outgoing Director Lisa Osofsky. Ephgrave brings a different background to the role, as a former assistant commissioner with the Metropolitan Police Service and not a career prosecutor or even lawyer. In February 2024, in his first public remarks since assuming the role, Ephgrave emphasized swift resolution of cases and a pragmatic new enforcement action strategy, including not being afraid to shut down investigations that do not appear likely to progress to charges. He also suggested the SFO may move to compensate whistleblowers, modelling off the U.S. example, and may make greater use of cooperating defendants (known as "assisting offenders" in the U.K. system) to obtain information in exchange for more lenient sentences, as permitted under the Serious Organized Crime and Police Act.

Time will tell if Director Ephgrave's bold pronouncements will yield more or swifter investigations, but his office will at least have some new advantages in doing so. In October 2023, the Economic Crime and Corporate Transparency Act 2023 became law, giving SFO prosecutors several tools in their efforts to investigate corporate fraud, though several of the law's changes for fraud cases already extended to corruption cases. These include a new strict liability offense for "failure to prevent fraud" (supplementing existing "failure to prevent" offenses); expansion of "Section 2A" information-demanding powers to cover fraud cases in addition to the existing bribery and corruption contexts; and most broadly, changes in the "identification doctrine." The latter development effectively reduces the level of control of a company that bad actors must have before imposing full corporate-entity liability. The previous standard imposed liability only where malefactors represented the "directing mind and will" of the company, while the new standard requires only "senior manager" involvement.

In comments delivered at a September 2023 symposium, SFO Chief Capability Officer Michelle Crotty highlighted the importance of her office's cross-border collaboration with international authorities in the cases against Airbus (in 2020, with U.S. and French authorities) and Glencore (in 2022, with U.S., Swiss, and Dutch agencies), which Crotty touted as the SFO's premier actions from the five-year tenure of outgoing Director Lisa Osofsky. Such collaboration appears to be a new cornerstone for the SFO, with Crotty noting that the new Director Nick Ephgrave "will also be – like Lisa – invested in maintaining and building the SFO's relationships both within the UK and overseas."

EU

With the 2024 Olympic Games on the horizon, France has launched an anti-corruption push into the games' organizing. France is the first host country to be operating under an "anti-corruption clause" included in its Olympic games contract. Incidentally, the 2024 Summer Games were awarded in 2017, the same year France adopted its anti-corruption law, Sapin II. The country has applied that law's obligations, which generally require companies to create anti-corruption compliance programs, to the Olympic organizing committee, which is

thus under the jurisdiction of the French Anti-Corruption Agency (AFA). The AFA and prosecutors have announced four inquiries into the awarding of contracts in connection with the games and the pay of their chief organizer.

As we've written about previously here, in 2023, the AFA also issued guidance regarding internal anti-corruption investigations jointly with the National Financial Prosecutor's Office (PNF). The guide includes recommendations for corporate compliance with the Sapin Act and the whistleblower-related obligations of the 2022 Waserman Act.

OECD

Romania and Croatia in 2023 became the 45th and 46th nations to sign onto the OECD Anti-Bribery Convention. Beyond agreeing to implement the standards for the criminalization of bribery required by the convention, both countries will now also participate in reviews from the OECD to assess priorities for combatting foreign bribery. While participating in the convention is a public step towards elevating anticorruption as a priority, it remains to be seen what changes to their enforcement efforts the nations will implement. At the least, practitioners and clients in these nations should be aware of the increased possibility of cross-border collaboration between the local enforcement agencies and U.S. authorities as a result of their joining the convention.

Latin America

Brazil received its "Phase 4" peer review in 2023, the first OECD assessment conducted in the country since 2014. Unsurprisingly, the report, compiled by assigned reviewer nations Colombia and the U.K., credited the landmark Odebrecht investigation and resolution while noting areas for further progress in order to sustain this success. Among these, the report highlighted the reviewers' opinion that Brazil's statute of limitations for foreign bribery is hindering enforcement efforts, with one long-running investigation yielding eight acquittals due to the statute. In Brazil, the statute of limitations applies to both the time to secure a conviction and to execute the sentence and is recalculated retrospectively based on the sentence actually imposed. Because sentences do not commence until a conviction has become final, after exhausting all appeals, and because that appeals process can take many years, the OECD report noted the difficulty in obtaining enforceable convictions. According to the report, Brazil had not to-date obtained any foreign bribery sanctions against individuals, in stark contrast to its recent enforcement actions against corporate entities.

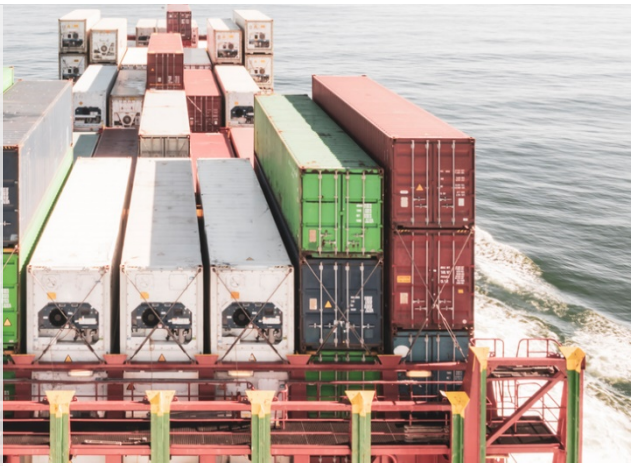
Also in Brazil, two recent decisions in December 2023 and January 2024 by Federal Supreme Court Justice Dias Toffoli have suspended fine obligations from leniency agreements entered into with J&F Investment (owner of meatpacking giant JBS) and Novonor (formerly Odebrecht). These decisions follow Justice Toffoli's September 2023 decision to annul substantial evidence from Operation Car Wash, which was implicated in both corporate resolutions, based on leaked messages from the operation task force that revealed purportedly improper cooperation between the prosecutors and a judge. Whether the evidentiary decision continues to yield ramifications for the myriad investigations stemming from Operation Car Wash remains an item to watch closely in 2024.

China

In July 2023, China launched a national campaign against corruption in the healthcare sector. The initiative, spearheaded by the National Health Commission and nine other government agencies, aims to tackle unethical practices in obtaining and paying for healthcare services, with specific emphasis on improper remunerations to hospitals and healthcare providers (HCPs). In addition to increased scrutiny and audits of hospitals and HCPs, government agencies have also sharpened their focus on pharmaceutical and medical device companies. The initiative has seen coordinated national and local government action, including through a credit evaluation mechanism maintained by the National Healthcare Security Administration, by which local governments can designate companies as "unethical," with implications for their eligibility to participate in government-run volume-based procurement systems. Entities active in China's healthcare space must remain vigilant in 2024 as this crackdown continues to unfold and should assess their compliance programs as enforcement activities ramp up.

In another development, in February 2024, China revised its state secrets law to expand the scope of information within its purview. The law now requires business entities to disclose to the government their "work secrets," a term which is not yet defined with specificity but encompasses items "that are not state secrets but will cause certain adverse effects if leaked." The latest legislative development expanding China's national security controls continues a trend going back at least a decade, with incremental developments—including last year's updates to the anti-espionage law—making external investigations and diligence more challenging and more fraught with potential investigations by Chinese authorities into domestic law violations.

ENFORCEMENT OF U.S. TRADE SANCTIONS AND EXPORT CONTROLS IN 2023 AND WHAT TO EXPECT IN 2024



by Shrutih Tewarie, Luciano Racco, Anthony D. Mirenda, Nicholas Alejandro Bergara, Amanda Gialil, Aleksis Fernandez Caballero, Zihan Mei and Chawkat Ghazal

Throughout 2023 and early 2024, we continue to witness deepening geopolitical and economic divides globally. The U.S. and its allies (most significantly the EU and the G7), spurred on by Russia's war in Ukraine, continue to engage in unprecedented coordination of their efforts to punish and technologically constrain adversaries. Sanctions, export controls, and other international trade laws have been central to these efforts. The targets are familiar: Russia, China, Iran, and North Korea. Robust enforcement will continue to be critical to the U.S. pursuit of its national security, foreign policy and economic objectives. In 2023, several U.S. government agencies collaborated not only on issuing enforcement guidance but also on notable enforcement actions. Both the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") and the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") imposed their highest penalties ever in 2023. In addition, BIS and the U.S. Department of Justice ("DOJ"), updated their respective voluntary self-disclosure ("VSD") policies, which, together with OFAC's preexisting VSD policy, are likely to spur additional disclosures and the resulting enforcement activity.

Actions taken over the past year and government priorities for 2024 ensure that businesses worldwide must remain vigilant and continue to focus on building and strengthening their international trade compliance programs. This blog post will focus on U.S. trade sanctions and export controls compliance and enforcement activity.

U.S. ENFORCEMENT ACTIVITY

The U.S. continues to press its "whole of government" approach to enforcement of U.S. trade sanctions and export controls, expanding their use to further U.S. foreign and economic policy objectives, providing additional guidance, increasing the incentives for voluntary self-disclosure and conducting robust investigation and prosecution efforts. As Russia's war on Ukraine persisted, and as terrorism and military conflicts flared across the Middle East and in Africa, many companies and individuals seen as aiding the military or economic interests of Russia, Iran or other adversaries have been targeted for enforcement actions. China, too, remains a focus of U.S. economic and national security concerns, and those involved in illicit technology transfers to China continue to face investigation and prosecution. The U.S. continues to focus on the serious risks (money laundering, sanctions evasion, and terrorism or other criminal finance, to name a few) presented by virtual currency and continues to press enforcement actions against individuals and companies operating in this space. Finally, U.S. government agencies expanded their collaboration efforts, jointly issuing enforcement and compliance guidance and cooperating on notable enforcement actions.

A. Tri-Seal Compliance Notes

Over the past year, the DOJ, OFAC, and BIS ("Agencies") jointly issued three Tri-Seal Compliance Notes outlining common approaches on several key topics.

First, in March 2023, the Agencies released a Tri-Seal Compliance Note ("March 2023 Note") identifying tactics used by bad actors involving third-party intermediaries to conceal transactions with SDNs, parties on the Entity List, or Russian end users. The Agencies highlighted these tactics "to assist the private sector in identifying warning signs and implementing appropriate compliance measures." Common red flags include transactions involving personal email accounts (as opposed to company accounts) or entities with minimal (or no) internet presence (e.g., website). In addition, private sector actors should be wary of customers who are reluctant to provide information regarding a product's end use or end user.

Second, in July 2023, as described in a previous client alert, the Agencies issued a Tri-Seal Compliance Note ("July 2023 Note") regarding the voluntary self-disclosure of potential violations of U.S. sanctions and export controls. The July 2023 Note outlined the Agencies' respective voluntary self-disclosure ("VSD") policies (as of the time of that publication) and built upon actions that were taken in 2023 by OFAC and BIS under their respective pre-existing VSD policies. The July 2023 Note describes many—but not all—of the same details about the VSD policies discussed below (in Section V.B), and also describes the whistleblower program implemented by the Financial Crimes Enforcement Network ("FinCEN").

Under the FinCEN whistleblower program, those who report to FinCEN (or the DOJ) violations that relate to U.S. trade and economic sanctions or the Bank Secrecy Act may receive a financial reward. If the whistleblower's report leads to a successful enforcement action, the potential award ranges from 10 to 30 percent of the money FinCEN (or the DOJ) obtains through the enforcement action. FinCEN is also open to rewarding whistleblowers who disclose information that leads to the enforcement of a "related action" (e.g., an action under the Export Control Reform Act). FinCEN's program will accept anonymous reports as well, although FinCEN states that such reports must be made through legal counsel.

Finally, in March 2024, the Agencies announced their first Tri-Seal Compliance Note of 2024 ("March 2024 Note") concerning the applicability of U.S. sanctions and export controls against non-U.S. individuals or entities in foreign countries or territories. The March 2024 Note describes the range of enforcement mechanisms available "for the U.S. government to hold non-U.S. persons accountable for violations of such laws, including criminal prosecution."

With respect to OFAC, the March 2024 Note provides illustrative examples of the type of conduct where OFAC would seek to penalize foreign persons, including, for instance, a scenario in which a non-U.S. person conducts an illicit transaction using the U.S. financial system that causes a U.S. financial institution to process a payment in contravention of OFAC sanctions.

With respect to BIS, the March 2024 Note makes clear BIS's position that "U.S. export control laws may extend to items subject to the EAR anywhere in the world and to foreign persons who deal with them." It goes on to reiterate that the EAR applies not only to the initial export of a product, but also to reexports, in-country transfers (e.g., within the foreign country), items with more than *de minimis* U.S. content, and products subject

to the various foreign direct product rules. The March 2024 Note also generally outlines recent DOJ, BIS, and OFAC enforcement actions that highlight how the Agencies have prosecuted non-U.S. persons who violate U.S. sanctions and export controls overseas. It concludes by providing compliance considerations for non-U.S. persons, including that such persons should develop and maintain internal trade compliance programs, institute comprehensive know-your-customer programs, and be ready to take action immediately and in an effective manner when compliance issues arise.

B. VSD Policy Updates

1. DOJ

DOJ continues to prioritize two main threats: (1) "the unlawful export of sensitive commodities, technologies, and services [which] pose a serious threat to the national security of the United States"; and (2) U.S. individuals and companies or organizations transacting with sanctioned individuals and entities. The DOJ's National Security Division (NSD) issued a revised VSD policy in early March 2023 addressing these threats, and highlighting incentives for companies to self-disclose as a way to reduce, and potentially eliminate, criminal liability when they have identified and notified potential criminal violations of U.S. sanctions and export control laws.

As discussed in a prior client alert, this VSD Policy confirms for the first time that where a company voluntarily self-discloses potentially criminal violations, fully cooperates, and timely and appropriately remediates the violations, NSD generally will not require the disclosing party to enter a criminal a guilty plea, and there will be a presumption that the company will receive a non-prosecution agreement and will not pay a fine. However, this policy is only applicable to those companies who disclose a potential violation to NSD "within a reasonably prompt time after becoming aware" of the possible infraction, in circumstances where the company does not already have a legal obligation to disclose, and when the voluntary disclosure occurs "prior to an imminent threat of disclosure or government investigation." If aggravating factors are present, such as a substantial profit from the misconduct or involvement by high-ranking executives, then the non-prosecution agreement presumption is inapplicable and DOJ would be able to pursue criminal prosecution. Moreover, in all circumstances, the company will be required to disgorge any funds gained from the underlying misconduct.

This VSD policy will only cover an entity if it has made its disclosure to NSD, so disclosures made only to other agencies, such as BIS and OFAC, will not qualify. Consistent with other VSD policies, the disclosing entity must share "all relevant non-privileged facts known at the time" and fully cooperate with NSD. Timely "cooperation" includes collecting and preserving relevant documents and information and identifying potential avenues of investigation for NSD.

To benefit from NSD's policy, the disclosing party must also "timely and appropriately remediate any violations." Notably, NSD will consider whether the party "implemented an effective and sufficiently resourced compliance and ethics program." NSD will also be considering whether the party imposed disciplinary measures, such as compensation clawbacks, with respect to employees who were involved in, or were supervising areas in the company connected to, the underlying misconduct.

2. BIS

In April 2023, BIS issued **guidelines** clarifying its policies regarding voluntary self-disclosures. Like the other agencies, these BIS guidelines were published to incentivize entities and individuals to self-disclose violations.

Unlike other agencies, though, BIS has used these guidelines to expressly focus attention on the disclosure of "significant" possible export control violations. That is, BIS has created a dual-track system to deal with VSDs: one that fast-tracks minor or technical violations and another that handles "significant" violations.

In the April 18 memorandum setting out the guidelines, BIS Assistant Secretary for Export Enforcement Matthew Axelrod ("Axelrod") described BIS's intention to affect the risk calculus of filing a VSD for significant violations, explaining that, filing a VSD could result in a substantially reduced—or even a fully suspended—penalty. A VSD must be timely, comprehensive, and involve full cooperation to qualify for a substantial reduction in the applicable civil penalty under BIS's base penalty matrix. Notably, filing a VSD will not alone guarantee a reduced penalty, but instead will be considered together with a company's forward-looking efforts to enhance its compliance program to prevent reoccurrence of the violation. Axelrod also highlighted that an entity's affirmative choice to not submit a VSD for a significant violation would be considered an aggravating factor in BIS's assessment of penalties.

Axelrod also explained that multiple minor or technical violations would be treated differently. BIS now advises that minor violations, if close in time, can be bundled into a single VSD. As stated in Axelrod's April 18 memorandum, "[w]e're not focused on increasing the number of minor or technical VSDs we receive… submit one overarching submission … to streamline the process on their end and conserve resources on ours." In most cases, BIS has indicated it will issue a warning or no-action letter in connection with minor or technical violations within 60 days of such a submission.

Further, BIS states that it will view the disclosure by one party (Party A) of a violation by another party (Party B) that leads to an enforcement action as an instance of "extraordinary cooperation." BIS asserts that it will consider that Party A made such a disclosure as a mitigating factor in any future enforcement action that may be brought against Party A, even for unrelated conduct. Understood literally, BIS would seem promising to "bank" a company's current good behavior (in the form of the disclosure of another entity's violations) against the disclosing company's future bad behavior. To the extent that this policy could be viewed as incentivizing future violations, this is likely not quite what BIS intended, but at a minimum, it seems that BIS seeks to reinforce the view that the making of such a disclosure is part of being an otherwise good corporate citizen, and would deserve receiving some benefit in the future.

The VSD policy appears to be having the intended effect. BIS recently announced that while the overall number of VSDs remained constant from 2022 to 2023, BIS received 80% more VSDs containing potential serious violations in 2023 than in 2022.

In January 2024, BIS released an additional memorandum describing steps to enhance the "efficiency and effectiveness" of its VSD program. In this memorandum, BIS strongly encouraged electronic submissions of VSDs. Additionally, BIS will now allow an abbreviated narrative account to describe the nature of violations that involve only minor or technical infractions under the "fast-track" resolution policy, so long as there are no aggravating factors present. In another effort to streamline the process for VSDs of minor violations, BIS will no longer require the full five-year lookback recommended in Section 764.5(c)(3) of the EAR, nor all of the accompanying documentation outlined in that Section, unless requested by the Office of Export Enforcement. In the memorandum, BIS indicated that if a party seeks to return an unlawfully exported item back to the US, BIS will presumptively authorize such a reexport (this has already been BIS's approach in practice).

3. OFAC

Like BIS and the DOJ, OFAC also encourages VSDs and has drafted similar policies to incentivize companies to self-disclose potential violations of U.S. sanctions. As noted in its Enforcement Guidelines (31 CFR Part 501), OFAC considers VSDs to be a mitigating factor in an enforcement action. In situations where a civil monetary penalty may be imposed, an OFAC VSD can result in up to a 50 percent reduction in the base amount of the proposed penalty. OFAC evaluates conduct described in a VSD using a totality of the circumstances approach, including for example, considering the party's compliance program (or lack thereof) and its effectiveness, as well as identifying whether the party has taken corrective action to address the possible violation.

C. Creation of Disruptive Technology Strike Force

As discussed in a previous client alert, in February 2023, the DOJ and the Department of Commerce launched the Disruptive Technology Strike Force. The Strike Force brings together experts from different government agencies, including the FBI, Homeland Security Investigations, and 14 U.S. Attorneys' Offices. The purpose of the Strike Force is to target illicit actors, strengthen supply chains, and protect critical technological assets from being acquired or used by nation-state adversaries. Its work will focus on investigating and prosecuting criminal violations of export laws, enhancing administrative enforcement of U.S. export controls, fostering cooperation with the private sector, and leveraging partnerships to coordinate law enforcement actions and disruptive strategies. The Strike Force also plans to strengthen its connections with the intelligence community.

D. Significant Enforcement Actions

1. DOJ

Last year, DOJ prosecuted several violations committed by foreign and domestic actors, in many cases involving U.S. adversaries and military end-users in China, Russia, Iran, and North Korea.

For example, a California resident was convicted of conspiring to ship aeronautics software to a Beijing university while contracted as a program administrator to a space science research nonprofit. The nonprofit had a contract with NASA to license and distribute Army flight control software, which the defendant sought to procure. In another instance, two U.S. Navy servicemembers were arrested and charged with "transmitting sensitive military information" to a Chinese intelligence officer. Some of this sensitive national defense information included technical manuals and key information on the "weapons, propulsion and desalination systems" used on certain U.S. Navy assault ships.

In cases involving Russian military end-users, two U.S. citizens were charged with violating U.S. export controls for a two-year scheme repairing, procuring, and shipping aviation-related technology headed to Russian end-users. In another elaborate conspiracy to procure and ship U.S. critical technologies for Russian military end-users, two Russian nationals were charged by the DOJ in a sophisticated procurement network using Brooklyn-based companies to buy goods on behalf of sanctioned end-users to support Russia's military. Similarly, the DOJ charged a Belgian national in two separate indictments for allegedly helping to illegally export military-grade technology from the U.S. to end-users in China and Russia. The Belgian national allegedly procured more than $2 million worth of sensitive technology, and worked with a U.S. resident to smuggle the items out of the U.S. The Belgian national was subsequently arrested in Belgium. And, in another high-profile prosecution, the DOJ charged former senior FBI official Charles McGonigal in connection with a scheme to violate U.S. sanctions by providing services to a sanctioned Russian oligarch, Oleg Deripaska.

In cases involving Iranian end-users, a dual citizen of Iran and the U.S. was sentenced to 30 months in prison for "conspiring to illegally export U.S. goods and technology to users in Iran, including the Central Bank of Iran." The defendant used two United Arab Emirates-based front companies to illegally purchase electronic goods and technology from American tech companies for Iranian end-users. Another Iranian national was also found guilty of violating U.S. export controls by illegally shipping electrical cables and connectors from the U.S. through Hong Kong, and ultimately to Iran. Two companies, Tawain-based DES International and Brunei-based Soltech Industry, were ordered to each pay a fine and serve a 5-year corporate probation term for conspiring to violate U.S. sanctions and export control laws by shipping U.S.-made goods, including a power amplifier and cybersecurity software, to Iran.

The DOJ charged five individuals from Iran, Turkey and the United Arab Emirates with violations of the Arms Export Control Act and the International Emergency Economic Powers Act for attempting to export U.S. technology to assist Iran's ballistic missile and UAV (drone) programs between 2005 and 2013. Moreover, a U.S. national received a four-year prison sentence for conspiring to violate U.S. sanctions law by providing financial services to the Iranian government. These financial services were used to aid other Iranian individuals and entities, including a co-defendant, who plotted to kidnap a journalist in the U.S. to quell dissent against the Iranian regime. Lastly, and in its first-ever criminal resolution involving the sale of Iranian oil, the DOJ secured a guilty plea from Empire Navigation for violating U.S. sanctions by facilitating the sale and transport of more than 980,000 barrels of Iranian oil.

2. BIS

In the "largest standalone administrative penalty in BIS history," BIS imposed a $300 million civil penalty on Seagate Technology LLC of Fremont, California and Seagate Singapore International Headquarters Pte. Ltd., of Singapore (collectively "Seagate") for violations of U.S. export controls related to Seagate's continued shipment of millions of hard disk drives to Huawei. Even after Huawei was placed on the Entity List for its conduct against U.S. national security interests and after Seagate's competitors stopped selling to Huawei, Seagate continued to sell hard disk drives to Huawei. The settlement identifies 429 violations of the EAR between August 2020 and September 2021. In addition to the financial penalty, Seagate will now be subject to a multi-year audit requirement.

As discussed in a previous client alert, in a coordinated effort, BIS and OFAC imposed a combined $3.3 million penalty against Microsoft Corporation for its apparent violations of U.S. sanctions and export controls involving conduct by its foreign subsidiaries. Although the violative conduct predated the sanctions and export controls imposed on Russia related to its war in Ukraine, Microsoft allegedly failed to ensure its compliance program was effective and current. Despite having self-disclosed the violations, BIS and OFAC imposed a substantial penalty due to the presence of aggravating factors including: (a) that the over 1,300 apparent violations (resulting from software licenses sold and services provided to SDNs, blocked persons and users in sanctioned jurisdictions) directly impacted U.S. foreign policy objectives; (b) the determination that Microsoft acted with "reckless disregard" for U.S. sanctions; and (c) the "substantial experience and expertise" Microsoft has in software transactions.

Additionally, BIS worked with DOJ to obtain guilty pleas from individuals attempting to smuggle weapons and sensitive material to foreign countries. Most notably, BIS worked with DOJ to obtain a guilty plea from a Rhode

Island man who purchased "ghost gun" kits and manufactured them into working firearms to be unlawfully exported to the Dominican Republic.

Finally, in an enforcement action alongside the DOJ and the State Department, BIS fined South Carolina-based 3D Systems Corporation over $2.7 million for committing multiple violations of the EAR, including violations of recordkeeping requirements. The company was found to have committed a range of export violations, including the illegal shipment of U.S.-origin aerospace blueprints and military electronics to China and controlled design documents to Germany. BIS highlighted that 3D Systems Corporation acted with "disregard" for its export compliance responsibilities, particularly by continuing to export the technical data even after discovering its own violations. The State Department's parallel enforcement action is discussed below in Section D.4.

3. OFAC

OFAC's enforcement actions broke records in 2023, generating civil monetary penalty/settlement amounts totaling over $1.5 billion. In total, OFAC brought 17 enforcement actions in 2023, with penalty and settlement amounts ranging from $31,000 to $968 million. Notably, most of the enforcement actions were brought against companies operating in the financial services (6 out of 17) and virtual currency (4 out of 17) sectors. Additionally, it appears that we will continue to see an increased coordination effort and alignment of enforcement priorities among OFAC and other agencies, including the DOJ, BIS, and FinCEN, as well as greater cooperation between the U.S., the EU, the UK, and other allies especially in the context of Russia sanctions. OFAC's most significant enforcement actions of 2024 are described below. Additionally, OFAC continued its efforts to target Russia's military and financial infrastructure and to enforce the Russian oil price cap by adding two new shipping entities and their registered vessels to the SDN List for violating the price cap policy.

British American Tobacco p.l.c.

The British American Tobacco p.l.c. ("BAT") enforcement action highlights the weight that aggravating factors (e.g., harm to national security or willful acts) can have on a penalty amount. BAT's Singapore subsidiary and a North Korean company established a joint venture company ("Joint Venture"). The Joint Venture was located in North Korea and had the purpose of manufacturing and distributing BAT cigarettes. The BAT subsidiary exercised effective control over the Joint Venture, holding a 60 percent stake, and supplied the Joint Venture with professional services, equipment, tobacco, and other material to produce cigarettes. BAT later directed the subsidiary to sell its stake in the Joint Venture to a Singapore-based trading group ("Singapore Company") for one euro, seeking to obscure BAT's continued effective ownership and control over the Joint Venture. Ultimately, twelve U.S. financial institutions processed several hundred USD payments from North Korea to the Singapore Company, including payments that were ultimately remitted to the BAT subsidiary. In addition, the BAT subsidiary, in partnership with the Singapore Company, also exported cigarettes to the North Korean Embassy in Singapore up through 2017.

BAT's conduct was found to have resulted in a violation of § 544.205(b) of the Weapons of Mass Destruction and Proliferators Sanctions Regulations and fifteen violations of § 510.212 of the North Korea Sanctions Regulations. OFAC identified five substantial aggravating factors, including (1) BAT management's willful conduct, knowing that U.S. sanctions prohibited the transactions but engaging in them anyway; (2) BAT's active concealment of facts surrounding the transactions, ignoring requests for information from banks and deleting references to North Korea from the information provided; (3) knowledge and participation by senior

management; (4) that BAT's misconduct enabled North Korea to establish a billion-dollar cigarette industry, thus materially helping the North Korean regime; and (5) BAT's size and sophistication. The enforcement action resulted in a settlement of $508 million to OFAC and $629 million to the DOJ. In the settlement, OFAC stressed that BAT's attempts to create the illusion of distance between the company and the violations was a significant aggravating factor. In addition, OFAC was highly critical of the ongoing failure by BAT's senior management to create and enforce a culture of compliance, to conduct risk assessments or implement an effective risk-based compliance program, and to adapt that program over time as the risks evolved.

Binance

On November 21, 2023, OFAC announced a historic $960 million settlement with Binance, a Cayman Islands company and the world's largest virtual currency exchange. The enforcement action and subsequent settlement resulted from Binance's apparent violations of Iranian, Syrian, North Korean, Ukrainian/Russian, and Cuban U.S. sanctions regimes between August 2017 and October 2022. Binance allegedly carried out virtual currency trades on its online exchange platform between U.S. persons and users in sanctioned jurisdictions or blocked persons. Binance also allegedly took steps to project an image of compliance but did so by misleading third parties about its controls. Senior Binance management knew of and permitted the presence of both U.S. and sanctioned jurisdiction users on its platform and did so despite understanding OFAC-administered sanctions programs.

The $968 million settlement amount was based on several aggravating factors, including the fact that Binance's violations were not self-disclosed and that the conduct was egregious. Specifically, OFAC determined that Binance knew, or likely knew, that its conduct would violate U.S. sanctions regulations and that Binance's senior management mischaracterized its commitment to sanctions compliance to third parties. Finally, OFAC also highlighted the fact that Binance was a "commercially sophisticated actor." The Binance settlement underscores the importance of establishing management commitment to sanctions compliance that is backed by adequate resources. For companies operating in the virtual currency industry, such as Binance, OFAC expressly indicates that compliance mechanisms should be incorporated into the company's platforms and systems, such as through "KYC [know-your-customer] protocols, transaction monitoring, sanctions screening, algorithmic configurations, and other controls as appropriate." Companies operating in this space should also be mindful that virtual currency exchanges existing outside of the United States should not cause U.S. persons to violate U.S. economic sanctions or result in the exportation of goods and services to sanctioned jurisdictions or blocked persons.

4. The U.S. Department of State Directorate of Defense Trade Controls ("DDTC")

In the past year, DDTC has also been active, imposing civil penalties for violations of the Arms Export Control Act ("AECA") and the ITAR in connection with unauthorized exports and retransfers of technical data.

In February 2023, as mentioned above, 3D Systems Corporation entered into a consent agreement with DDTC in connection with unauthorized exports and retransfers of technical data to various countries, including China. 3D Systems Corporation was fined a total of $20 million (with $10 million suspended on the condition that this amount be applied to remedial compliance costs as outlined in the Consent Agreement) and was required to appoint a designated Special Compliance Officer for the entire term of the Consent Agreement, in addition to conducting two audits during this period. DDTC credited extensive cooperation and 3D Systems' agreement to take significant steps to improve its compliance program as the reason DDTC did not issue a debarment.

In April 2023, VTA Telecom Corporations ("VTA") entered into a consent agreement with DDTC in connection with both unauthorized exports and attempted exports of defense articles, including technical data to Vietnam. DDTC asserted that the violations were willful, including false statements as to the items involved and the end use, and the conduct was discovered as the result of a DOJ criminal investigation including the execution of a search warrant at the company. Pursuant to ITAR §127.7(a), VTA was administratively debarred for a period of 3 years, and thereby prohibited from participating directly or indirectly in any transaction subject to the ITAR. VTA must then submit a request for reinstatement after the expiration of the debarment period, subject to DDTC approval, before resuming such transactions.

In August 2023, Island Pyrochemical Industries Corp. entered into a consent agreement with DDTC in connection with its unauthorized brokering in connection with the transfer of ammonium perchlorate from a Chinese company to a company in Brazil, using false statements on license applications. Island Pyrochemical agreed to pay $850,000 (with a potential $425,000 suspended on the condition that it be applied to specified compliance costs). Compliance measures included in the agreement include the appointment of a designated Special Compliance Officer, an independent audit, and strengthening compliance policies, procedures, training, and an automated export compliance system.

Most recently, in February 2024, the Boeing Company ("Boeing") settled with DDTC in connection with unauthorized exports to China and violations of DDTC license terms and conditions. As a result, DDTC imposed a $51 million penalty (with $24 million suspended on the condition that this amount will be used towards remedial compliance measures outlined in the Consent Agreement). Boeing has consented to two audits in addition to strengthening its compliance policies, procedures, and training, which will be implemented under the supervision of a Special Compliance Officer for the entire term of the Consent Agreement.

OUTLOOK FOR 2024

Enforcement activity across the whole of government, including DOJ and the Departments of State, Treasury and Commerce, was extraordinarily active over the past year. BIS and OFAC both had record-breaking years in 2023, and neither shows any signs of slowing down. Indeed, both OFAC and BIS obtained some of the highest—or in the case of BIS's Seagate action, the highest—penalty and settlement amounts in their respective histories. Moreover, given the significant number of interagency collaborations on enforcement, it is expected that the agencies will continue coordinating efforts to maximize their respective resources and investigate and prosecute potential violations from multiple angles.

Developments in international trade law continue to gather pace overwhelming both regulators and regulated entities. Those responsible for ensuring compliance with an ever-increasing number of legal requirements must keep abreast of changes to the law and modify their compliance programs accordingly. Foley Hoag's international trade and national security group regularly assists companies of all sizes seeking to navigate international trade laws.

CONGRESSIONAL INVESTIGATIONS: A REVIEW OF INVESTIGATIONS LIKELY TO CONTINUE IN 2024 AND INTO THE 119TH CONGRESS

by Veronica Renzi, Matthew E. Miller and Eli Greenspan

In an election year, Congress tends to shift focus away from legislating on Capitol Hill as the approaching elections take center stage. Instead of regular legislative order, companies should be prepared for Congress to focus on and potentially intensify investigations in both chambers.

Below we outline numerous areas of investigative interest where Congress has acted in the previous year, in addition to emerging areas where Congress could seek information and testimony from private sector entities, particularly U.S. companies with connections to China, companies leveraging artificial intelligence, social media companies, the pharmaceutical industry, firms that have publicly announced ESG policies or practices, and fossil fuel companies.

China

On the heels of introducing the BIOSECURE Act in December 2023, the House Select Committee on the Chinese Communist Party (CCP) is working with several other committees to investigate Chinese ties to US-based companies and foreign companies operating in the U.S. Given the rising geopolitical tensions with China, this will continue to be an area of intense focus and sensitivity for U.S. lawmakers.

In January 2024, the House Homeland Security Committee accelerated its joint investigation into cybersecurity vulnerabilities in the U.S. maritime sector and supply chain risks. The Committee requested information from a Swiss company, which works with a Chinese state-owned enterprise accounting for nearly 80 percent of the ship-to-shore cranes at U.S. maritime ports, for information on its commercial relationship with the company and to describe their work with U.S. government agencies involved in defense, intelligence, and other U.S. national security elements. The Committee has been exploring this relationship throughout 2023 to better understand Chinese software capabilities used in cranes, some of which are remotely operated and employ technology that could track container information. Cybersecurity threats to critical infrastructure are a top priority for government officials and are likely to remain a top priority due to heightened concern over China's cybersecurity activities in the United States.

Also in January, the House Energy & Commerce Committee launched an investigation into federal grants made to an artificial intelligence (AI) scientist at the University of California, Los Angeles (UCLA) with alleged ties to the CCP. The letter sent to UCLA puts the responsibility on higher education entities to prevent foreign adversaries from receiving highly sensitive U.S. research funded in whole or in part by federal government grants. Congressional interest in artificial intelligence picked up rapidly in 2023 and is expected to continue as

the federal government operationalizes plans across each federal agency to understand the challenges and opportunities of artificial intelligence.

In February, the House Select Committee on the CCP unveiled findings from a bipartisan investigation of five U.S. venture capital firms. The investigation found that these firms had invested billions in AI and semiconductor companies with ties to China. Given the overlapping issues and national security interests, congressional investigations into entities with connections to China will likely continue.

ESG Practices

The widespread adoption of environmental, social, and governance (ESG) practices has become an increasingly hot topic on Capitol Hill. House Republicans charge that ESG practices from private companies push non-material social goals that undermine public markets and lead to increased costs for consumers. In addition to introducing several anti-ESG bills, such as a bill aimed at preventing the Securities and Exchange Commissions from requiring companies to disclose their carbon emissions, several House committees have launched investigations into investment firms they accuse of violating antitrust laws. The House Judiciary Committee, led by Rep. Jim Jordan (OH), accuses these companies of potentially violating antitrust laws by deploying ESG policies in their investment portfolios in ways that may restrict investments in coal, oil, and gas.

Energy Infrastructure Projects

In fall 2023, two top Republican lawmakers sent a letter to the Department of Energy's Loan Programs Office seeking information on its relationship with cleantech businesses. This office is a public financer of high-impact energy projects and manufacturing investments, with a focus on clean energy and supply chain projects. The $400 billion office has been subject to intense focus from Congress in the past but has received new interest since the passage of the Inflation Reduction Act, which expanded the types of projects eligible for financing.

Medicare Advantage

In September 2023, the U.S. Senate Committee on Finance Chair Ron Wyden (D-OR) and the House Committee on Energy & Commerce Ranking Member Frank Pallone (D-NJ) announced a bicameral investigation into managed care plans' prior authorization practices. The Committee action follows a U.S. Department of Health and Human Services (HHS) Office of the Inspector General report on Medicaid Managed Care Organizations (MCOs) utilization of prior authorization. Letters were sent to numerous health plans and insurers requesting information on prior authorization practices.

Congress has taken a direct interest in health insurers and a variety of business practices that impact access, costs, and outcomes. Congress's interest in artificial intelligence will also keep attention on stakeholders leveraging artificial intelligence systems across the healthcare industry.

Pharmaceutical Pricing

Drug pricing has been a consistent focus for lawmakers that has consisted of Congressional hearings, investigations, and legislation like the Inflation Reduction Act, which authorized HHS for the first time to engage in negotiations for certain prescription drugs. The Senate Committee on Health, Education, Labor and Pensions (HELP), led by Sen. Bernie Sanders (I-VT), has focused on prescription drug costs this Congress, holding numerous hearings on the cost of insulin and inhalers, and released two committee reports related to pharmaceutical pricing and compensation. The Committee recently held a hearing in January after inviting

four companies to testify and requesting information and documents on internal decisions regarding inhaler pricing and access.

While these investigations have thus far been partisan, aspects of the work are undoubtedly of interest to both parties.

Drug Shortages & Supply Chain

Throughout 2023, Congress debated how to address drug shortages for cancer drugs and other common medications like Adderall, which received national news. In September 2023, the House Energy & Commerce Committee held a hearing on drug shortages, exploring ways to strengthen the supply chain to prevent such disruptions. Legislation to confront this crisis is still pending, but Congress' interest in the issue will continue due to the intensity of coverage for certain products, like cancer drugs, in shortage that can lead to worse outcomes for patients who cannot access needed medicine. In January, the Senate Finance Committee released a white paper on a plan to prevent generic drug shortages, which explores several issues and entities across the supply chain that could be subject to future reforms.

In February 2024, Democrats on the House Oversight Committee launched an investigation into drug shortages, requesting information from companies to better understand the root causes and practical solutions to addressing persistent drug shortages. While this investigation seems to be more focused on collecting information, the collection of documents and other information could raise new questions or lead to further action. The Federal Trade Commission (FTC) and HHS are also soliciting public comments on the root causes of and potential solutions to drug shortages and may launch their own investigations soon.

Private Equity and Health Care

Private equity companies' activities span several sectors, so it is notable that the Senate Budget Committee launched an investigation into the impact of private equity ownership on America's hospitals. In December 2023, the Committee launched a bipartisan investigation into the effects of private equity ownership on U.S. hospitals. The inquiry explores whether various financial transactions may have impacted the quality of care for patients in hospitals under such ownership. Other committees have highlighted private equity ownership of healthcare facilities, which could spell further action in the future.

Higher Education

Universities will continue to draw Congressional inquiries this year, given the bipartisan outrage at several prominent universities handling of antisemitism on their respective campuses last year. Rep. Virginia Foxx (R-NC), Chair of the Committee on Education and the Workforce, requested follow-up information from Harvard University in January 2024 regarding Harvard's response to antisemitism on campus. The House Ways and Means Committee launched a similar inquiry, noting many higher education institutions' 501(c)(3) tax-exempt status and whether these institutions are complying with anti-discrimination laws. This high-stakes inquiry and the potential tax treatment implications make this one to closely watch in the coming year.

Social Media

Congressional interest in social media companies cuts across several issues, specifically the impact on youth mental health, as well as privacy and censorship concerns. The House Judiciary Committee has an open investigation into concerns over censorship by social medical companies and whether there has been any

coordination with the federal government to censor speech. The Senate Judiciary Committee recently held a hearing on online child sexual exploitation. There are several bills in both chambers to address challenges posed by social media, a sign that Congressional interest is growing.

In election years, expect lawmakers on both sides of the aisle to closely scrutinize social media companies for how they police disinformation and artificial intelligence that could sway voters in key states or districts. Both parties have shown interest in understanding how social media companies can prepare, prevent, and police such information. Following the last election, Facebook was asked to turn over thousands of politically themed advertisements to the Senate Intelligence Committee bought through Russian accounts during the 2016 presidential election.

Closing Thoughts

Foley Hoag is closely tracking the dynamic landscape of Congressional investigations as we get into the second session of the 118th Congress. As these issues play out and new issues emerge, we emphasize leveraging our best practices for navigating these inquiries. For companies wary of potential Congressional scrutiny or aware of the risks operating in these industries, it is important to consider the evolving political landscape, the priorities of the Biden Administration, and those lawmakers poised to ascend into new roles with investigative authority in the 119th Congress.

MASSACHUSETTS' NEW ATTORNEY GENERAL – A LOOK BACK AND A LOOK AT THE YEAR AHEAD

by Rachel Kerner, Rosie Loring and Jeremy W. Meisinger

Last year, Foley Hoag reviewed what we could expect from the Office of the Massachusetts Attorney General ("OAG") as Attorney General Andrea Campbell took on her first year in office. This post examines whether the initiatives identified by the new administration at the start of her term were actually prioritized and whether we expect to see continued development in those areas this year.

Elder Law

While campaigning, Attorney General Campbell vowed to form the Elder Justice Unit and focus on using the office's tools to protect Massachusetts elders from hardship caused by unequal access to health care, deceptive business practices, and fraud.

In August 2023, AG Campbell announced the creation of that unit, appointing Mary Freeley as director. The new unit is charged with convening internal and external elder justice groups to listen to priorities and ongoing issues, enhancing the existing work of the office to prosecute the abuse and exploitation of vulnerable older adults, working with the OAG's Community Engagement Division to conduct intentional outreach to elders, and advocating for state and national policy that aligns with and advances the work of the Elder Justice Unit. One of the unit's first steps was to launch a free hotline for elders to call in regarding a range of issues.

While Attorney General Campbell made good on her promise to create the Elder Justice Unit, the unit itself seems still to be ramping up on the enforcement front. For example, OAG's recent prosecution of a Medicaid consultant for stealing from elderly nursing home victims was prosecuted by the Medicaid Fraud Division.

Reproductive Justice

As with the Elder Justice Unit, AG Campbell promised the creation of a Reproductive Justice Unit and a renewed focus on reproductive justice and rights at the start of her term. OAG fulfilled these campaign promises. In October, AG Campbell announced Sapna Khatri to lead the newly created Reproductive Justice Unit, which will focus on "ensuring that Massachusetts is a national leader on reproductive justice by expanding and protecting access to reproductive and gender-affirming care, addressing disparities in maternal health, tackling misinformation and disinformation that prevents access to care, working across state lines to respond to national attacks on reproductive health care, and championing and defending Massachusetts' strong legal protections for reproductive rights."

The Reproductive Justice Unit has taken its mission to heart, and its undertaking remains a core focus of OAG.

For example, in the spring of 2023, AG Campbell announced a $1.5 million maternal health grant program aimed at reducing maternal health disparities and promoting culturally competent care. In August, AG Campbell awarded $1.5 million to 11 organizations as part of the grant expanding access to culturally competent group models of prenatal care, perinatal behavioral health support, and breastfeeding support.

We expect that as reproductive justice and rights continue to play an important role nationally—particularly during election season—the Reproductive Justice Unit and action in this space will continue to be a priority of the OAG.

Gun Safety

As promised at the outset of 2023, gun safety has emerged as a high priority of both the Office and AG Campbell herself. Some highlights include:

- AG Campbell filing a multi-state amicus brief to uphold laws restricting gun magazine capacity;
- AG Campbell urging the ATF to expand background checks and reduce illegal gun trafficking, co-leading a coalition of 21 attorneys general in support of a proposed ATF rule that would broaden firearms sales license requirements and expand the background check requirements for buyers;
- AG Campbell co-leading a coalition of 20 attorneys general in filing an amicus brief in the Ninth Circuit, arguing that states can restrict ownership of weapons of war consistent with the Second Amendment;
- OAG successfully defending the Commonwealth's law banning assault weapons in *Capen and National Association for Gun Rights v. Campbell*, where the District of Massachusetts denied plaintiffs' request to block the state's ban on the sale and possession of assault weapons and large capacity ammunition magazines;
- AG Campbell joining a multi-state coalition calling for federal action to stop the sale of military-grade ammunition used in mass shootings.

In addition, in November 2023, AG Campbell announced a new Gun Violence Prevention Unit, naming Christine Doktor as Director and Ryan Mingo as Deputy Director. The Unit is tasked with enforcing the Commonwealth's gun and consumer protection laws, working to ensure that Massachusetts has the strongest, most comprehensive commonsense firearm laws in the country, supporting the defense of commonsense gun laws from legal challenge and supporting law enforcement, and community-based gun violence prevention work to help reduce gun deaths and shootings across the Commonwealth. While Massachusetts has one of the lowest rates of gun violence in the nation, the gun violence in Massachusetts disproportionately affects Black youth. The Unit seeks to address this disparity. Moreover, recognizing the direct connection between public health and public safety, the Unit will seek to support both community-based and law enforcement violence prevention efforts by providing training and technical assistance on gun law compliance and by exploring potential grant programs to bolster community violence prevention and to support survivors and their families.

Given the creation of the Unit just a few months ago and OAG's proactive action related to gun safety nationwide, we can expect this area to remain very active in the coming year.

Access to Education

AG Campbell campaigned on Access to Education as a key priority to her leadership and we noted last year that her first month in office showed a commitment to this issue. The following months proved this through demonstrating that AG Campbell remains focused on addressing issues facing students including predatory lending, DE&I, and loan repayment.

In October, AG Campbell joined Governor Healy in issuing joint guidance to affirm and strengthen equality efforts in higher education and K-12 schools. Issued in response to the Supreme Court's decisions in *Students for Fair Admissions, Inc. v. President and Fellows of Harvard College* and *Students for Fair Admissions, Inc. v. the University of North Carolina*, the guidance focuses on admissions standards and access issues in higher education while providing guidance for promoting equality in K-12 schools to facilitate future success.

AG Campbell also collaborated with Boston Mayor Michelle Wu this year in hosting a student loan forgiveness clinic to help federal student loan borrowers navigate the Public Service Loan Forgiveness program. The effort saw U.S. congressional support, with Senator Elizabeth Warran and Congresswoman Ayanna Pressley joining the clinic. The clinic is part of an ongoing effort by the OAG's Student Loan Assistance unit to help borrowers access debt relief programs by offering ongoing webinars for borrowers.

The OAG has also signaled a commitment to using its enforcement efforts and amicus briefs to further its Access to Education goals. In October, AG Campbel led a coalition of 23 attorneys general in a multi-state amicus brief supporting strong relief options for borrowers harmed by predatory lending, and in September, AG Campbell co-led a letter to the Biden administration expressing concerns regarding potential loan servicing programs.

Opioid Crisis, Labor Violations, and Health Care

In last year's post, we identified the opioid crisis, labor violations, and health care as areas on which we expect AG Campbell to continue to focus. Those areas have seen activity over the last year, with labor violations emerging as a key focus under AG Campbell's leadership.

In November 2023, AG Campbell announced the indictment of an alleged $1.6 million Medicaid fraud scheme, and in August, the OAG announced a $2.6 million settlement with an ambulance company to resolve false billing allegations.

This year, AG Campbell partnered with several law enforcement agencies resulting in major opioid take-downs. In March, the OAG announced the significant arrest and recovery of more than two and a half kilograms of fentanyl in partnership with the State Police under the New England Fentanyl Strike Force and in September, OAG partnered with the State Police and several local law enforcement agents to execute the takedown a major fentanyl trafficking operation across the Merrimack valley.

Historically, Massachusetts has been a leader in pursuing healthcare violations and opioid enforcement efforts. As these high-profile efforts indicate, we expect these areas to continue to be active.

Additionally, labor violations have emerged in the last year as a major priority of the OAG under AG Campbell, including actions related to labor trafficking and wage and hour violations. In a recent interview, for example,

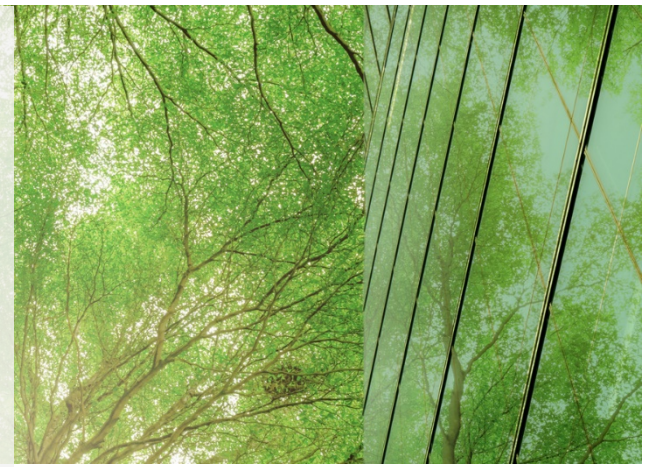
Campell reiterated that labor was one of the biggest challenges facing Massachusetts residents. In that interview she vowed continued aggressive enforcement efforts against employers or contractors "not willing to pay their workers" and noted that the office's prioritization of violations of child labor laws.

Efforts in this space are not limited to enforcement actions. AG Campbell's first year indicates a commitment to policy advocacy on labor issues. In May, the OAG filed an amicus brief before the U.S. Court of Appeals for the First Circuit in the case *Patel v. 7-Eleven* interpreting Massachusetts independent contractor statute. AG Campbell's lawsuit challenging the Occupational Safety and Health Administration (OSHA)'s decision to roll back the public reporting requirements resulted in OSHA's reversal of this position and adoption of a robust rule to protect worker safety.

* * *

The first year in office demonstrated the OAG's commitment to many of AG Campbell's campaign promises, especially in gun safety, reproductive justice, and access to education. Labor violations emerged as an additional area of focus. We can expect to see continued prioritization of these areas in Campbell's second year in office. In addition to these priorities, across industries, Campbell's office is giving increased scrutiny to issues affecting vulnerable populations, including immigrants, elders, children, women, the LGBTQ community and low-income residents.

TENNESSEE V. BLACKROCK: HOW THIS CASE INFORMS HOW WE LOOK BACK AND LOOK AHEAD AT ESG



by Matthew E. Miller and Jasmine N. Brown

Politicians in Republican-led states have painted a target on environmental, social, and governance (ESG) principles being employed as a metric for investments. About one year ago, in March 2023, twenty-one Republican Attorneys General sent a letter to asset managers, including BlackRock, Inc., asserting breaches of their fiduciary duties and violations of antitrust law as a result of the asset managers' ESG investing and participation in efforts to increase public company disclosure around the risks and impacts of climate change.

Whatever the effectiveness of the AG attacks related to ESG in the political arena (the consideration of which is beyond the scope of this article), a recent consumer protection action filed by one of those Attorneys General – Tennessee Attorney General Jonathan Skrmetti – against Blackrock suggests that actually asserting those fiduciary breaches and antitrust violations may not be viable as a legal matter.

In this article, we will examine the broad attacks set forth in the March 2023 Republican Attorneys General letter and compare them to the claims asserted in the Tennessee case against asset manager Blackrock, Inc. The Tennessee AG has pivoted to a consumer confusion claim based on what he contends are mixed messages about ESG investing, suggesting a future path for other state officials interested in pursuing actions against asset managers to follow.

March 2023 Letter to Asset Managers

On March 30, 2023, 21 Republican Attorneys Generals sent a letter to over 50 U.S. asset managers, including BlackRock, Inc., putting forth several "concerns about the ongoing agreements between asset managers to use Americans' savings to push political goals during the upcoming proxy season." The letter targets the managers' participation in efforts such as Net Zero Asset Managers ("NZAM") and Climate Action 100+ ("CA100+"), which push for more detailed and consistent disclosures regarding greenhouse gas emissions and the risks posed by climate change for the benefit of investors.

Essentially, the letter raises the following four categorical allegations:

1. Asset managers participating in NZAM and CA100+ are in breach of their fiduciary duties of care and loyalty unless they disclose to investors that all of their funds are "ESG funds," regardless of whether they are designed and marketed as such.

2. Asset managers have failed to properly disclose the risks associated with funds marketed as ESG funds, because "ESG funds perform poorly," while managers charge higher fees for managing those funds.
3. Asset managers who engage with companies to encourage them to disclose "non-material" climate change risks are breaching their fiduciary duty of loyalty because doing so will "destroy value and make companies and their investors worse off," and these requests are being instigated by "radical ESG activists" with a "political agenda" and "routinely try to change company behavior through shareholder resolutions."
4. Participation in NZAM and CA100+ may "unreasonably restrain trade and harm competition" in violation of antitrust law.

Tennessee Lawsuit Against Blackrock

Of the twenty-one AGs who signed onto the March 2023 letter, to date, one has filed a legal action against an asset manager concerning ESG investing. On December 18, 2024, Tennessee Attorney General Jonathan Skrmetti brought a consumer protection action against BlackRock seeking injunctive relief, civil penalties, disgorgement, restitution, and costs. But while the March 2023 letter made sweeping allegations of breaches of fiduciary duty and violations of antitrust law, Skrmetti does not make those claims in his complaint. Instead, he alleges that BlackRock has confused Tennessee consumers by saying that it both seeks to maximize investment returns and focuses on minimizing environmental impact, which Skrmetti believes to be incompatible. The allegations in the Tennessee lawsuit boil down to an assertion of mixed messages by Blackrock which may lead to consumer confusion. Blackrock must file a response to the Tennessee complaint by May 17, 2024, which many will no doubt read with interest.

While Tennessee AG's legal theory is a far cry from the allegations in the March 2023 letter, it suggests a pathway the other AGs who signed onto the March 2023 letter may follow. Montana Attorney General Austin Knudsen, joined by several other Attorneys General, has recently cited the allegations made in the Tennessee complaint as cause for continuing investigation into Blackrock, with potential additional enforcement activity to follow[1]. And Mississippi Secretary of State Michael Watson also issued a cease-and-desist order against BlackRock on March 27, 2024, mimicking in large part the consumer protection allegations raised in the Tennessee action[2]. Claims of consumer deception in the ESG space will thus be an area to continue to watch as we move through 2024 and beyond.

[1] Press Release, Montana Attorney General, Attorney General Knudsen Investigating BlackRock's ESG Policies, Conflicts Of Interest (Mar. 1, 2024), https://dojmt.gov/attorney-general-knudsen-investigating-blackrocks-esg-policies-conflicts-of-interest/; Letter from Austin Knudsen, Montana Attorney General, to BlackRock Fund Directors (Feb. 27, 2024), https://dojmt.gov/wp-content/uploads/Follow-up-letter-to-BlackRock-Directors-FINAL.pdf.

[2] Press Release, Mississippi Secretary of State, Mississippi Secretary of State Issues Order Against BlackRock for Alleged Securities Fraud Related to ESG Investment Strategy with Possible Multimillion-dollar Penalty (Mar. 27, 2024), https://www.sos.ms.gov/press/mississippi-secretary-state-issues-order-against-blackrock-alleged-securities-fraud-related; Summary Cease and Desist Order and Notice of Intent to Impose Administrative Penalty, In re BlackRock Inc., et al., Admin. Order No. LS-24-6726 (Mar. 26, 2024).

CRIMINAL TAX ENFORCEMENT – WHAT TO LOOK FOR IN 2024

by Matthew E. Miller and Jack C. Smith

IRS enforcement activity remained strong in 2023, with the volume of investigations and prosecutions initiated holding steady from 2022. Despite the substantial funding boost provided by the Inflation Reduction Act, with some $79.6 billion flowing to the IRS over the next 10 years—much earmarked for enforcement—enforcement staffing is still historically low. For example, while overall staffing at IRS Criminal Investigation ("IRS-CI") has increased modestly over the past two years (up 4% over 2022), it remains nearly 22% lower than the staffing levels of 2010 (see recent IRS annual Data Books and IRS-CI Annual Reports). So while we may fairly expect to see a further staffing bump in 2024, any further effects translating this into enhanced enforcement may take longer yet to materialize.

According to the IRS-CI's 2023 Annual Report ("2023 Annual Report"), the agency continues to dedicate its resources primarily to tax investigations (69.9% of agent time), in accordance with IRS-CI's status as the only federal law enforcement agency with jurisdiction to investigate federal tax crimes. Among other areas commanding attention, narcotics-related investigations stand out with 11.3% of investigative time, demonstrating the broad scope of financial crimes handled by the agency and the high priority placed on narcotics across the federal law enforcement landscape.

Several trends emerge from a review of the 2023 Annual Report and the enforcement actions highlighted by the agency.

National Security

IRS-CI has a prominent role in national security initiatives, including sanctions-related initiatives that have carried over from our preview of 2023 trends. In a separate announcement from May 2023, IRS-CI announced it had 23 sanctions-related investigations ongoing.

Task Force KleptoCapture continues to target Russian oligarchs and other high-priority sanctions evaders. IRS-CI has also provided blockchain-analysis training and tools to Ukrainian law enforcement.

And clearly mindful of attention towards the ongoing conflict in Gaza, IRS-CI specifically called out "past disruptions of terrorist organizations like Hamas," without noting any specific ongoing Hamas-related investigations. This suggests that IRS-CI may be scrutinizing the region for opportunities to become involved.

Energy-Credit Abuses

IRS-CI has focused on various fuel credits in 2023. First, it highlighted the Fuel Tax Credit (FTC), a longstanding credit intended for off-highway businesses and farms, as a frequent vehicle for unscrupulous promotion of tax refunds to individuals via inapplicable credits. IRS-CI noted a "significant" increase in individual returns claiming the FTC and a corresponding uptick in FTC-related investigations implicating $164 million in potentially fraudulent credits.

While the FTC has been part of the tax code for decades, investigations into abuse of such credits have expanded to include renewable energy credits, such as in the prosecution of five individuals in connection with a $1 billion biofuel conspiracy centered on Utah biodiesel company Washakie Renewable Energy—touted by the agency as one of the largest fraud schemes in U.S. history.

Demonstrating focus on the energy space, IRS-CI also investigated a scheme seeking to defraud a tax-free renewable-energy grant program funded through the American Recovery and Reinvestment Act of 2009.

Looking ahead, the 2021 Bipartisan Infrastructure Law and the Inflation Reduction Act, cornerstones of President Biden's legislative agenda to date, have earmarked $97 billion in funding for the Department of Energy in part to establish and expand similar renewable-energy grant programs. Participants in such grant programs should be keenly aware of IRS scrutiny of their grant submissions and the potential for IRS-CI enforcement, even beyond the traditional scope of "tax" investigations.

Darknet and Cybercrime

While the IRS has long been involved in investigating financial cybercrime, several initiatives this year highlight the growing resources dedicated to this expertise. IRS-CI highlighted the continuing emphasis on investigations involving digital assets, leveraging partnerships with the private sector to investigate techniques such as chain-hopping and token-swapping.

This cyber expertise can be particularly important in the cutting-edge enforcement against darknet marketplaces, which IRS-CI has recognized in organizing existing resources to support a Cyber-Organized Crime Drug Enforcement Task Force (Cyber-OCDETF) to focus on investigations involving the darknet and virtual currencies.

Additionally, IRS-CI and partners from another task force (the Joint Criminal Opioid and Darknet Enforcement task force) announced a major takedown in Operation SpecTor, resulting in 288 arrests (and seizure of substantial amounts of narcotics and firearms) relating to alleged crimes involving cryptocurrency and darknet marketplaces. Coordinated takedowns of this nature require substantial collaboration across enforcement agencies and thus serve as a public pronouncement of the investigating agencies' priorities.

In June 2023, IRS-CI announced a pilot program in which it is sending four IRS-CI agent "cyber attachés" around the globe to collaborate with local law enforcement in Australia, South America (specifically, Bogota, Colombia), Asia (Singapore), and Europe (Frankfurt, Germany). These long-term assignments supplement IRS-CI's existing 11 foreign attaché postings around the globe.

Again in June 2023, IRS-CI also joined with other federal agencies to launch the Darknet Marketplace and Digital Currency Crimes Task Force. The proliferation of these task forces highlights the increasing emphasis on cross-agency collaboration, particularly when operating in complex and cutting-edge subject areas.

COVID-19 Relief Programs

Among the individual enforcement actions called out by the 2023 Annual Report, frauds implicating various COVID-19 relief—whether through the CARES Act, Paycheck Protection Program, or relief programs for businesses or individuals—remain a standout contributor to the bottom-line case statistics and show no signs of slowing down. While the names of the government programs may change, one thing remains constant: whenever a government program broadly disburses new funds or credits to the public, IRS-CI will play a prominent role in closely scrutinizing associated filings for low-hanging fruit.

Syndicated Conservation Easements

Intended as a charitable tax deduction to promote the conservation of open land, conservation easements—and particularly the "syndicated" variety involving multiple investors in a pass-through entity that purchases a single plot of land to be conserved—have recently been in IRS-CI's crosshairs as a vehicle for purportedly fraudulent tax shelters. In addition to pushing Congress for reform of this credit, the IRS has brought significant enforcement actions in this space, including the noteworthy case against Jack Fisher and his associates. As highlighted in the 2023 Annual Report, Fisher was found guilty in September 2023 of running a scheme in which he and his associates backdated investor buy-ins and allegedly inflated the value of easements so that high net worth investors could claim unmerited deductions.

The government alleged that Fisher conspired with his CPA, attorney, and land-appraiser co-defendants to sell stakes in landholding entities to wealthy investors, with the subject land being appraised in some cases for more than 10 times what Fisher's companies had paid for it. After taking in investors, sometimes *after* the close of the tax year, the entities donated conservation easements on the land. Given the appraised values, the investors were able to claim substantial tax deductions above their cash investments. Following a lengthy trial, the jury convicted Fisher and an attorney co-defendant, James Sinnott. In January 2024, Fisher was sentenced to 25 years in prison for his role in leading the scheme to sell over $1.3 billion in fraudulent deductions, while Sinnott was sentenced to 23 years. Importantly, beyond the inflated-appraisal conduct, Fisher and Sinnott were both implicated in more traditional fraudulent conduct to support the scheme, including backdating documents for submission to the IRS.

Notably, one of the appraisers who had worked with Fisher, Clayton Weibel, was acquitted. One lesson from this split verdict may be that a high appraisal ratio and the argument that deductions were "too good to be true" will not alone carry the day for the government in a criminal case where its burden includes proving a mens rea requirement, while the presence of more traditionally fraudulent conduct may make for a stronger case to a jury. Nonetheless, practitioners in this space should proceed with caution, as the two convictions and eight guilty pleas obtained in connection with Fisher's scheme—including two post-trial pleas in January 2024—may embolden the Department of Justice and IRS-CI to continue to bring such cases in the criminal system, despite the Weibel acquittal.

Regardless of the specific impact of the Fisher case, though, the existing syndicated conservation easement regime is nearing its end. Long a target of the IRS, syndicated conservation easements have been legal for many years. But as part of the federal omnibus spending legislation enacted in late 2022, Congress passed a provision that limits deductions for investors in syndicated conservation easements to 2.5 times their investment. This apparent compromise permits some legitimate investment in promoting conservation while attempting to curtail the disproportionate returns offered by abusive tax shelters. Charles Rettig, IRS Commissioner until November 2023, characterized the deduction cap as "critical to the ongoing efforts of the IRS to stem the tide of abusive syndicated conservation easements." The legislation gives the IRS a new enforcement tool, as it has promised to "ensur[e] compliance with the conservation easement deduction law as amended . . . and will continue to scrutinize transactions that are 'too good to be true.'" The IRS is now working on operationalizing this new tool, as in November 2023, the agency announced proposed implementing regulations that include explanations, definitions, and guidance on statutory exceptions and calculation methods. Time will tell if the new limit on profit has the impact the IRS sought on only the truly fraudulent schemes or whether it will prove a heavy-handed response that chills legitimate conservation.

For more information on Foley Hoag's 2024 White Collar Year in Preview Series, please contact your Foley Hoag attorney or the following contacts:

Caroline Donovan
Partner – *Boston*
+1.617.832.1252
cdonovan@foleyhoag.com

Anthony Mirenda
Partner – *Boston*
+1.617.832.1220
amirenda@foleyhoag.com

Shrutih Tewarie
Partner – *New York*
+1.212.812.0333
stewarie@foleyhoag.com

Yoni Bard
Associate – *Boston*
+1.617.832.3061
ybard@foleyhoag.com

Aleksis Fernandez Caballero
Associate – *Boston*
+1.617.832.1239
afernandezcaballero@foleyhoag.com

Chawkat Ghazal
Associate – *Boston*
+1.617.832.1198
cghazal@foleyhoag.com

Jace Lee
Associate – *New York*
+1.212.812.0336
jalee@foleyhoag.com

Leah Rizkallah
Associate – *Boston*
+1.617.832.3059
lrizkallah@foleyhoag.com

Christopher Escobedo Hart
Partner – *Boston*
+1.617.832.1232
chart@foleyhoag.com

Veronica Renzi
Partner – *Washington, DC*
+1.202.261.7316
vrenzi@foleyhoag.com

Jeremy Meisinger
Counsel – *Boston*
+1.617.832.3029
jmeisinger@foleyhoag.com

Nicholas Alejandro Bergara
Associate – *New York*
+1.212.812.0415
nbergara@foleyhoag.com

Susanna Chi
Associate – *Boston*
+1.617.832.3107
schi@foleyhoag.com

Amanda Gialil
Associate – *Boston*
+1.617.832.1103
agialil@foleyhoag.com

Rosie Loring
Associate – *Boston*
+1.617.832.1779
rloring@foleyhoag.com

Jack Smith
Associate – *Boston*
+1.617.832.1119
jcsmith@foleyhoag.com

Matthew Miller
Partner – *Boston*
+1.617.832.3041
mmiller@foleyhoag.com

Madeleine Rodriguez
Partner – *Boston*
+1.617.832.1720
mrodriguez@foleyhoag.com

Luciano Racco
Counsel – *Washington, DC*
+1.202.261.7319
lracco@foleyhoag.com

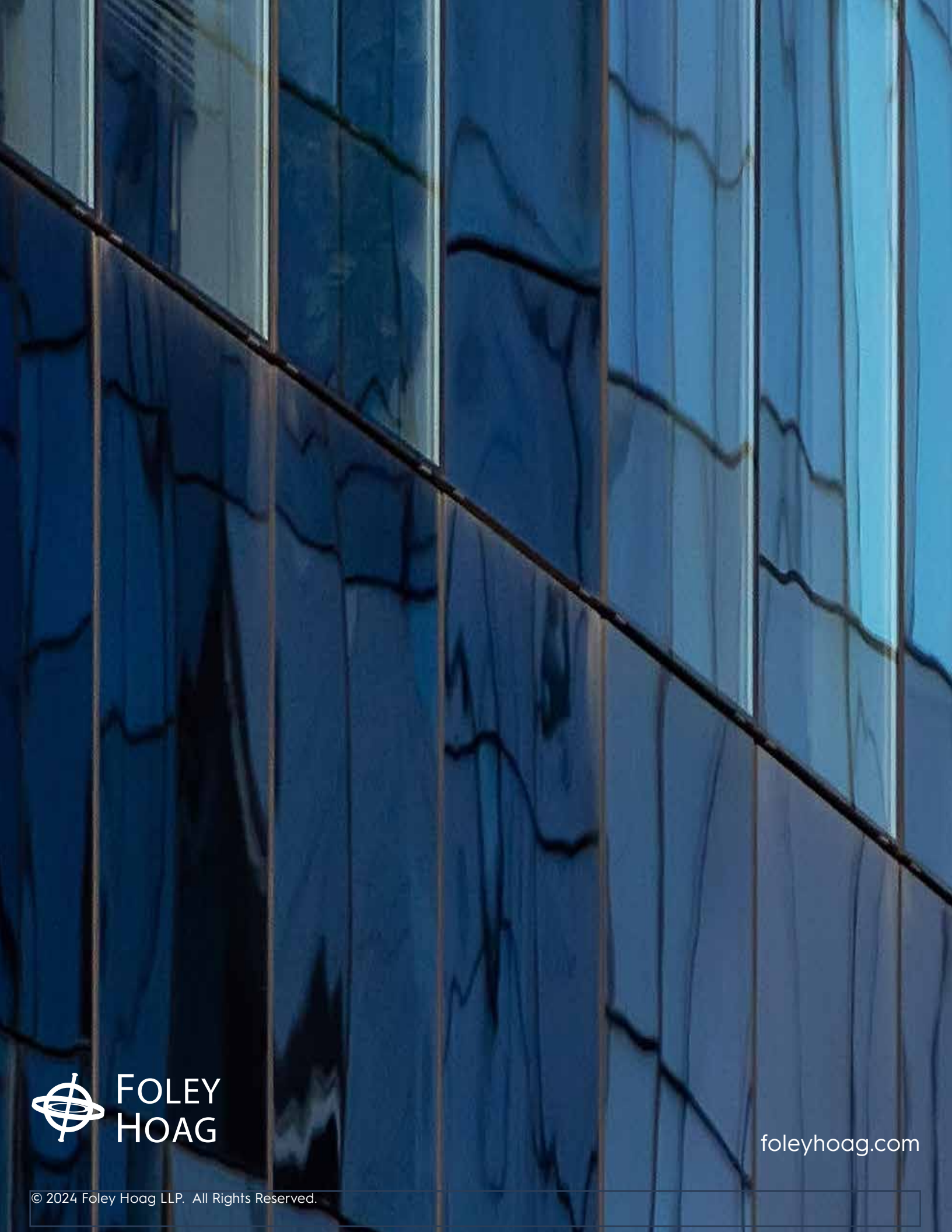
Jasmine Brown
Associate – *Boston*
+1.617.832.3123
jnbrown@foleyhoag.com

Christian Garcia
Associate – *Boston*
+1.617.832.1256
cgarcia@foleyhoag.com

Rachel Kerner
Associate – *Boston*
+1.617.832.1253
rkerner@foleyhoag.com

Zihan Mei
Associate – *Boston*
+1.617.832.1711
zmei@foleyhoag.com

Eli Greenspan
Policy Advisor – *Washington, DC*
+1.212.261.7326
egreenspan@foleyhoag.com



FOLEY HOAG

foleyhoag.com