FOLEY HOAG

2026 WHITE COLLAR YEAR IN PREVIEW

FOLEY HOAG WHITE PAPER

APRIL 2026

FOLEYHOAG.COM

FOLEY HOAG

2026 White Collar Year in Preview Series

April 2026

FOLEY HOAG THOUGHT LEADERSHIP

TABLE OF CONTENTS

2026 HEALTH CARE FRAUD YEAR IN PREVIEW

BY CAROLINE DONOVAN, YONI BARD, DAVID G. LAZARUS, NATALIE PANARIELLO, DALTON SOUSA, ISABEL CELIO

One year into the second Trump administration, we have seen a continuation of some evergreen enforcement priorities as well as new fonts of potential risk and exposure. As in years past, the investigation and prosecution of health care fraud cases remains at the forefront of the federal government's enforcement activity, though tempered by the government's interest in a variety of non-health care enforcement, some of which we take up in forthcoming entries in our Year in Preview series.

ENFORCEMENT HIGHLIGHTS IN 2025

As of the date of publication, the U.S. Department of Justice had not yet released judgment and settlement data in False Claims Act cases, including health care cases. Some charged conduct from 2025, however, provides a glimpse at metrics showing another big year for health care fraud enforcement. In particular, on June 30, 2025, the Justice Department announced the results of the National Health Care Fraud Takedown, charging 324 defendants in connection with over $14.6 billion in alleged fraud. This wide spanning enforcement action was a combined effort of 50 federal districts and 12 state Attorney General's Offices across the United States. The charges encompassed a broad range of alleged schemes, including kickbacks and bribery arrangements; telemedicine and durable medical equipment billing; opioid distribution and prescription fraud; pharmacy and compounded drug claims; fraudulent wound care services; home health and hospice billing telemedicine; and laboratory and genetic testing fraud.

As part of this takedown, the government brought Operation Gold Rush, charging members of a transnational organization with over $10 billion in alleged health care fraud under a variety of theories, including kickbacks, medical necessity, and billing practices in telemedicine, laboratories, and durable medical equipment. These individuals have not yet been brought to trial in the United States.

The National Health Care Fraud Takedown is in line with an increased focus on eliminating barriers between different governmental groups that focus on health care fraud enforcement to bring cases more efficiently and with the benefit of pooled resources. We will continue to monitor developments in matters charged as part of this 2025 takedown.

STRUCTURAL CHANGES IN FEDERAL HEALTH CARE ENFORCEMENT

2025 saw various structural changes to the health care fraud enforcement landscape at the federal level. Perhaps most significantly, on May 9, 2025, Michael Granston stepped down as Deputy Assistant Attorney General for the Civil

Division's Commercial Litigation Branch, a role he had held since 2019 (and before that, various other roles at DOJ). On May 21, 2025, Brenna Jenny, a former partner at Sidley Austin focused on the False Claims Act, was announced as the new Deputy Assistant Attorney for the Commercial Litigation Branch. She is the first political appointee to hold the position.

Pivoting to July of 2025, the Trump administration reestablished the DOJ-HHS False Claims Act Working Group, pledging it is "fully committed to supporting such work" and encouraging whistleblowers to report false claims and potential fraud, waste, abuse, and mismanagement. This coincides with the May 2025 expansion of the Criminal Division's Corporate Whistleblower Awards Pilot Program to include federal health care benefits. Of note, that pilot expressly states that its coverage extends to "health care fraud schemes involving private insurance plans," a sign of the government's continuing efforts to expand the ambit of the alleged fraud on the government purse.

Meanwhile, in Massachusetts, the Justice Department expanded its Health Care Fraud Unit's New England Strike Force to the District of Massachusetts. This increased presence brings more federal enforcement resources to Boston, one of the nation's most significant health care and life sciences hubs.

While not strictly focused on health care, DOJ has also established an Enforcement & Affirmative Litigation Branch to establish proactive enforcement and high-impact affirmative litigation to enforce federal laws and regulations while bringing suit against states, municipalities, and private entities that it contends interfere with or obstruct federal policies. This branch is wide-ranging in scope and jurisdiction, including over FDA-related enforcement.

Still other changes are underway that may impact health care enforcement. On January 8, 2026, the Trump Administration announced the creation of the National Fraud Enforcement within the Department of Justice. In announcing the new division, the Administration cited its efforts "to end Minnesota's fraud epidemic," including with respect to alleged Medicaid fraud, among other forms of alleged fraud. It remains to be seen to what extent this new division concerns itself with health care fraud, given its diffuse focus, and likewise, to what extent other states in political tension with the Trump administration will be the focus of its enforcement activity.

AGENCY AND DEPARTMENT ACTIONS

One of the most significant announcements in 2025 came in May, when CMS stated it would be expanding its audit of Medicare Advantage plans as part of the government's intensified focus under the current administration to reduce what the government estimates is billions of dollars in overbilling every year. CMS currently has a backlog of several years' worth of audits it has not completed. Going forward, CMS plans to stay current on these audits by reviewing all Medicare Advantage plans annually. In addition, CMS announced its plan to complete, by early 2026, outstanding audits from payment years 2018 through 2024. CMS's plans include increasing the volume of records reviewed in each audit, from 35 records per health plan per year to as many as 200. To meet this substantial increase in volume, CMS planned to dramatically increase its ranks of medical coders, who manually verify diagnoses to ensure accuracy, by a factor of 50 during 2025 – from 40 coders to 2,000. This intensified scrutiny of Medicare Advantage plans

will likely lead to increased referrals to enforcement agencies.

In November 2025, CMS finalized changes to hospital price transparency regulations in CY 2026 Hospital Outpatient Prospective Payment System and Ambulatory Surgical Center Final Rule (CMS-1834-FC). Among other key changes, the regulations require that hospitals make public certain payment metrics, including 10th percentile, median, and 90th percentile allowed amounts. Further, hospitals are required to attest that they have included all standard charge information required pursuant to § 180.50, and, where applicable, all payer-specific negotiated charges in dollars. These revisions were effective January 1, 2026, but CMS has delayed enforcement until April 1, 2026 to allow hospitals time to implement the changes and systems to do so.

On December 4, 2025, CMS announced the ACCESS (Advancing Chronic Care with Effective, Scalable Solutions) Model, which will model and test a new payment approach marrying technology-supported care for patients with a variety of chronic conditions. Meanwhile, in collaboration with the ACCESS Model, the FDA announced on December 5, 2025 its Technology-Enabled Meaningful Patient Outcomes (TEMPO) for Digital Health Devices Pilot. The pilot was developed by the FDA's Center for Devices and Radiological Health in order to "pilot[] an approach to encourage the use of digital technologies that meet people where they are," per Commissioner Makary. The pilot is intended to establish improvements in outcomes for patients with cardio-kidney-metabolic, musculoskeletal, and behavioral health conditions. How this increased reliance on technology-supported care and digital health technologies is enforced remains to be seen.

And while HHS had dominated headlines for a variety of other reasons, there has yet to be much enforcement-related activity coming out of the department. This includes under the Administrative False Claims Act, which was amended at the end of 2024 as part of the Servicemember Quality of Life Improvement and National Defense Authorization Act (NDAA) for Fiscal Year 2025. While the Administrative False Claims Act promised a more streamlined path to resolve certain claims administratively (where DOJ opts not to prosecute and up to a $1 million threshold), we have yet to see reports of any such enforcement by HHS, CMS, or FDA.

HEALTH CARE FRAUD IN THE COURTS

We report below on some of the more significant health care fraud cases decided in 2025. We saw a mix of significant appellate decisions, touching on multiple health care fraud issues, and trials, a few of which we highlight below.

Reported Decisions

United States v. Clay, Nos. 23-3923 & 24-3038 (6th Cir. Dec. 19, 2025)

In United States v. Clay, the Sixth Circuit delivered a mixed but defense-friendly message for 2026: health care-fraud restitution is limited to actual loss and the enforcement of Mandatory Victims Restitution Action ("MVRA") apportionment.

Kevin Clay co-founded Theramedical, a pharmaceutical sales company that specialized in compounded prescriptions. At the district court, Clay was convicted of health care and tax fraud in connection with pattern of conduct where patients received from the company a portion of the insurance reimbursement on each prescription they filled.

While Clay's conviction survived review, the panel vacated significant restitution awards. The Sixth Circuit found the district court erred when it included medically necessary prescriptions in the restitution award. Because the only goal of the MVRA is to return victims to the status quo, the Sixth Circuit held that medically necessary claims are not a "loss" and cannot be included in the restitution order. The decision also provides guidance on apportionment of restitution among co-defendants, and further bars restitution based on acquitted tax conduct where the conduct is not part of the "scheme, conspiracy, or pattern of criminal activity."

United States v. Mattia, No. 24-2589 (3rd Cir. Oct. 21, 2025)

In October 2025, the Third Circuit joined the Fifth and Eleventh Circuits in holding that implicit misrepresentations in prescription claims can constitute fraud under 18 U.S.C § 1347.

In Mattia, the government alleged that a sales representative collaborated with a doctor, who independently signed off on expensive compounded prescriptions for specific patients without a legitimate doctor-patient relationship and without any examination. The sales representative then submitted these prescriptions to the company's insurance plan, earning commission from any medication prescribed. The district court dismissed the indictment, holding that there were no false statements in the prescriptions or the submitted insurance claims and where the representative was not himself included on the prescriptions or claims.

On appeal, the Third Circuit reversed, validating implicit misrepresentation theories in connection with prescription claims. The panel recognized implicit misrepresentations in both the prescriptions and in insurance claims that incorporated those prescriptions, finding that the indictment adequately alleged falsity. This expansion and acceptance of implicit misrepresentation claims in health care fraud thus continues, with particular implication for those prescribing in less traditional doctor-patient settings, including telehealth.

United States v. Schena, No. 23-2989 (9th Cir. July. 11, 2025)

In July 2025, in Schena, the Ninth Circuit interpreted for the first time the Eliminating Kickback in Recovery Act (EKRA), analyzing the provision criminalizing the payment of "remuneration . . . to induce a referral of an individual to a recovery home, clinical treatment facility, or laboratory." 18 U.S.C. § 220(a)(2)(A).

The case stemmed from more than $77 million in claims billed to private and public insurers by a lab alleged to have made payments to marketing intermediaries to induce various referrals for certain unnecessary allergy tests. At trial, the defendant was convicted. On appeal, the Ninth Circuit affirmed, holding that such payments to third-party marketing intermediaries are proscribed by EKRA and that the evidence at trial supported the defendant's conviction. With respect to the issue of percentage-based compensation, the panel "conclude[d] that a percentage-based compensation structure for marketing agents, without more, does not violate 18 U.S.C. § 220(a)(2)(A)." But the panel went on to conclude that percentage-based compensation will violate EKRA when, as in Schena, the defendant pays the marketing agent "to have him unduly influence doctors' referrals through false or fraudulent representations about the covered medical services."

Omni Healthcare, Inc. v. MD Spine Solutions LLC, d/b/a MD Labs Inc. ("MD Labs"), No. 25-1110 (1st Cir. Dec. 1, 2025)

In December, in *Omni Healthcare, Inc. v. Md Spine Solutions LLC*, the First Circuit affirmed the district court's grant of summary judgment in favor of defendant. (Our review of the district court decision can be found here). On appeal, the First Circuit agreed that MD Labs did not submit false Medicare claims "knowingly" under the False Claims Act, 31 U.S.C. § 3729(a)(1)(A).

The First Circuit examines in detail the scienter standard and the evidence before it. In relevant part, relator Omni Healthcare alleged that MD Labs submitted claims for more expensive PCR urine tests were not "reasonable and necessary" for tests ordered by Omni Healthcare clinicians. The First Circuit held that "in FCA cases alleging Medicare fraud based on laboratory testing, generally a laboratory can rely on a doctor's order to show that the test is "reasonable and necessary" under 42 U.S.C. § 1395y(a)(1)(A)," after which the burden shifts to the relator to rebut this showing. Or, as the panel put it, "the doctor's order for medical testing will generally offer a safe harbor of medical necessity that, once raised, a relator must rebut, discredit, or undermine to raise a genuine dispute of material fact as to the lab's scienter." Given MD Labs had in-hand test requisition forms from Omni Healthcare providers, the court declined to find that MD Labs acted with the requisite intent.

The decision will be helpful to lab defendants and others who can borrow from the panel's explication of the scienter standard.

Trials

United States ex rel. Bassan v. Omnicare, Inc (CVS/OmniCare), No. 1:15-cv-04179 (S.D.N.Y. July 7, 2025)

CVS/OmniCare is a prime example of the DOJ's promise to continue vigorous health care enforcement under the FCA. After a four-week trial, the jury found Omnicare, the largest long-term care pharmacy in the country, liable for fraudulently dispensing drugs to individuals in assisted-living facilities without valid prescriptions. The jury determined that OmniCare had billed government payors more than $135 million for false claims, yielding trebled damages against the company of more than $400 million – plus another $542 million in statutory penalties for the more than 3.3 million false claims submitted. DOJ touted this as "one of the largest damages verdicts rendered by a jury in a False Claims Act case." Omnicare's parent company, CVS Health Corporation, was also found liable for causing Omnicare to submit some of these false claims. The companies have appealed the verdict.

While the appeals remain pending, the outcome in this case at the district court underscores the government's appetite for pursuing prescription-validity theories under the FCA against long-term care pharmacies and affiliated entities involved in the claims submission process. The case sends a cautionary message to long-term care pharmacies about the importance of evaluating governance, controls, and oversight of billing and dispensing practices.

United States ex rel. Behnke v. CVS Caremark Corp., No. 14-cv-824 (E.D. Pa. June 25, 2025)

In another qui tam action, a relator alleged that CVS Caremark Corp. ("Caremark"), the pharmacy benefits manager (or PBM) of CVS Health Corp., violated the FCA by causing a

Medicare Part D plan sponsor, Aetna, to misrepresent in reports to the government the amounts Aetna had paid for prescription drugs on behalf of Medicare beneficiaries. That is because Caremark was allegedly charging Aetna more than other insurers for the same Medicare Part D drugs – and more than what Caremark was required to reimburse for filling Part D drug prescriptions, leading to overbilling of Medicare. Caremark was found liable following a bench trial and was ordered to pay trebled damages of $285,000,000 and civil penalties totaling $4,873,500. Caremark has appealed the decision.

This case is rare instance in which a PBM was not only named a defendant in an FCA case but also found liable. And since the case was filed in 2014, the government has shown increasing hostility toward PBMs and the alleged lack of transparency into their pricing models as reducing drug costs has gained traction as a bipartisan issue. The outcome speaks to the importance of ensuring that reported Part D costs match actual amounts reimbursed to pharmacies with controls that detect and prevent differentiation between plan-sponsor reporting and reimbursements to pharmacies for the covered drugs.

United States ex rel. Devarapally v. Ferncreek Cardiology, P.A, No. 5:17-cv-616-FL (E.D.N.C. Dec. 12, 2025)

In another FCA case, a North Carolina jury returned a verdict for the defendant, who was had been accused by a whistleblower of performing medically unnecessary procedures on cardiac patients. This defense victory, particularly following the government's intervention in the case, was a notable loss for the government but demonstrates that medical necessity cases remain a priority for both federal and state enforcement.

United States ex rel. Taylor v. Healthcare Associates of Texas, LLC, No. 3:19-cv-02486-N (N.D. Tex. Feb. 26, 2025)

A rather significant FCA case came out of the U.S District Court for the Northern District of Texas in *Healthcare Associates of Texas.* Following a jury trial, the defendants were found liable for overbilling Medicare by submitting claims that violated various Medicare rules and ordered to pay nearly $450 million in (trebled) damages and penalties. The defendants successfully challenged the award as excessive and unconstitutional, convincing the district court to slash the figure to approximately $16 million to avoid a damages figure that, applied under the FCA's per-claim penalty scheme, would have been grossly disproportionate under the Eighth Amendment.

This case shows that although relators can successfully try non-intervened FCA cases, and courts may uphold large claim counts and damages, courts may also limit civil penalties based on the argument that they vastly outweigh harm. This creates more complexities – and opportunities – for addressing damages following a jury verdict.

United States v. Gary Cox (DMERx CEO), No. 1:23-cr-20271 (S.D. Fla. June 6, 2025)

In Cox, the government alleged that Gary Cox, the CEO of the internet platform DMERx – together with certain pharmacies, telemedicine companies, and durable medical equipment suppliers – carried out a kickback-driven scheme to generate physician's orders for DME and to cause the submission of false and fraudulent claims to federal health care programs. A jury convicted the CEO of conspiracy to commit health care fraud and wire fraud (of over $1 billion) and other charges related to fraud and kickbacks. This case drives home the importance of ensuring compliance in

vendor and partner relationships, using controls and oversight for automation tools involved in health care billing, and having bona fide physician-patient interactions, including in the telehealth context.

United States v. Brody et al., No. 3:24-cr-329 (N.D. Cal. Nov. 18, 2025)

In *Brody*, the CEO and clinical president of a California-based digital health company were charged with conspiracy to commit health fraud for the submission of false and fraudulent claims for reimbursement of internet-based Adderall sales. The defendants allegedly charged individuals a monthly subscription fee in exchange for providing them easy access to Adderall and other stimulants. The defendants were convicted by a jury in November 2025, which conviction they have appealed. This case emphasizes DOJ's eagerness to pursue telehealth companies for platform-enabled drug distribution without adequate medical necessity or proper screening.

2026 ENFORCEMENT PRIORITIES

We review areas of focus in 2025 that we expect will maintain or increase in focus in 2026.

Artificial Intelligence

The increasing prevalence and sophistication of AI tools will likely increase health care fraud risk for companies that adopt them and supercharge enforcement activities by the government that leverage similar technology. Businesses across the country are rapidly adopting AI tools, and health care companies are no exception. But while these tools offer increased efficiency and improvements to service delivery, their use by health care providers may draw additional scrutiny from the government. For example, on August 20, 2025, DOJ announced that it had entered into a non-prosecution agreement with a provider in North Carolina to resolve a criminal investigation into an alleged health care fraud and identify theft scheme involving AI. Troy Health, Inc., according to the non-prosecution agreement, used an AI-powered health care management platform it developed to help obtain new Medicare Advantage enrollments, offering kickbacks to pharmacies that submitted enrollment referrals through the platform.

Use of AI, even by well-intentioned health care companies, could increase the risk of errors within the care delivery process that may implicate health care fraud laws. For instance, an AI tool used to determine the medical services or devices needed by a patient, if it generates errors, could lead to fraud allegations based on lack of medical necessity. AI-enhanced software used to apply diagnostic or procedural codes could generate erroneous coding, triggering improper billing to government payors and False Claims Act enforcement risks. Healthcare companies using AI may opt to implement certain human reviews and controls, given the risk that blind reliance on an AI tool known to hallucinate or make other kinds of mistakes could constitute "reckless disregard" and satisfy the FCA's scienter requirement.

The government is also using AI to streamline and enhance its work on the enforcement side. In announcing its 2025 National Health Care Fraud Takedown, DOJ boasted its creation of a Health Care Fraud Data Fusion Center, gathering expertise from across various federal agencies "to leverage cloud computing, artificial intelligence, and advanced analytics to identify emerging health care fraud schemes." Around the same time, the House Oversight Committee shared in a press release similar comments by Cybersecurity, Information Technology, and Government Innovation Subcommittee

Chairwoman Nancy Mace (R-S.C.) regarding the government's adoption of AI tools to increase enforcement: "Federal agencies are using AI to detect fraud before it happens — by using the technology to identify patterns of fraudulent behavior and working proactively to prevent improper payments."

Wound Care

The wound care sector can expect intensified scrutiny in 2026. Federal reimbursement of wound care products has exploded in recent years, which the government has attributed to how these products have been priced. In an October 31, 2025 press release, CMS reported that "Medicare spending on wound care products known as 'skin substitutes' has had unprecedented growth, rising from $256 million in 2019 to over $10 billion in 2024," and asserted that "[t]his dramatic spending increase is largely attributed to abusive pricing practices in the sector, including the use of products with limited evidence of clinical value."

As government spending on skin substitutes has increased, so has its fraud enforcement. DOJ announced on December 12, 2025 that, in what DOJ hailed as "the first prosecution of its kind," a married couple owning several wound graft companies in Arizona was sentenced to lengthy prison terms for causing a staggering $1.2 billion of fraudulent claims to be submitted to Medicare and other payors for grafts that were not medically necessary. According to DOJ, Alexandra Gehrke and Jeffrey King owned and operated companies that paid purported sales representatives to locate elderly Medicare beneficiaries in Arizona with any type of wound, many of whom were in hospice. Gehrke and King then allegedly directed these sales representatives to order "expensive bioengineered skin substitutes – amniotic membrane allografts made from human placental tissue," in the largest sizes available (regardless of the wound size) to be applied to the wounds, to maximize reimbursement. In doing so, the defendants allegedly directed nurse practitioners to suspend their own medical judgment and apply all skin grafts ordered by the sales representatives, even where such grafts were not medically necessary, resulting in grafts being applied in problematic scenarios (e.g., multiple grafts on the same wound, grafts applied where there was no wound, and grafts applied to terminally ill patients on palliative care).

Gehrke and King allegedly collected more than $600 million from federal and commercial payors on fraudulent claims. Additionally, Gehrke allegedly received over $279 million in illegal kickbacks from a wholesale graft distributor, in exchange for ordering the grafts, much of which she used to pay illegal kickbacks to sales representatives. In addition to their criminal sentences and restitution obligations for hundreds of millions of dollars, the owners agreed to pay $309 million to resolve civil False Claims Act cases brought by whistleblowers. These FCA cases remain under seal while the government continues to investigate other parties allegedly involved.

Leading up to the sentencing of Gehrke and King, there had been other enforcement activity in the wound care space. CMS announced in the October 31 press release that in 2025, its Fraud Defense Operations Center (FDOC) blocked nearly $185 million in payments to "suspect providers" billing for wound care products. Among those providers was one medical practice group that, as identified by CMS in September 2025, billed more than $4.3 million almost entirely for wound care treatment supposedly provided to one individual for whom there was no evidence of prior wound treatment. On November 21, 2025, DOJ announced a $45 million settlement with

Vohra Wound Physicians Management LLC, one of the largest wound care providers for patients in nursing homes and skilled nursing facilities, and others based on allegations that they violated the FCA by billing Medicare for medically unnecessary surgeries and other procedures. One of the government's allegations was that Vohra "programmed its electronic health record and billing software to ensure that Medicare was always billed for the higher-reimbursed surgical excisional procedure and to create false medical record documentation to support the scheme." This settlement shows that wound care practices, physician groups, and affiliated management entities can expect scrutiny not only of medical necessity but also the integrity of their billing models.

This year also brought monumental changes to federal reimbursement for skin substitutes. Beginning January 1, 2026, CMS shifted away from using the complex average sales price (ASP) reimbursement system to a dramatically lower, standardized rate for skin substitutes. CMS predicts that this change will reduce Medicare spending on skin substitutes by around 90%. It may also influence fraud enforcement activity. Previously submitted claims under the ASP system may undergo further review, particularly where the size, product used, or wastage had a material impact on the reimbursement. The new, simplified reimbursement regime will focus inquiries on more basic questions of medical necessity, product selection, and coding, rather than the accuracy of ASP calculations. Following years of high federal spending on reimbursements and headline-grabbing takedowns, pre- and post-2026 wound care claims will remain a hot spot for health care fraud enforcement.

Labs

Recent enforcement actions underscore the government's sustained focus on laboratories, a trend that likely continues in 2026. In 2025, the government resolved several matters involving genetic testing and drug testing in which laboratories and related actors allegedly submitted or caused the submission of false claims for testing without legitimate medical necessity or proper physician orders. In addition to these negotiated resolutions, the United States and the states of Georgia, Colorado, and South Carolina obtained a $114.5 million judgment arising from a cancer genetic testing laboratory scheme. The government alleged that marketers and lab operators orchestrated a nationwide operation to enroll beneficiaries in genetic cancer screening that was not medically necessary, often utilizing telemarketing pipelines and referral arrangements to generate test volume. The judgment highlights the significant financial exposure that can result when laboratories and their affiliates engage in mass-marketing models without individualized medical decision-making.

Telemedicine and Digital Health

Telemedicine and digital health likewise will remain a top DOJ enforcement priority. In the National Health Care Fraud Takedown described above, 49 defendants were charged in connection with the submission of over $1.17 billion in allegedly fraudulent claims to Medicare resulting from telemedicine and genetic testing. For example, in the Southern District of Florida, prosecutors charged an owner of telemedicine and durable medical equipment companies for allegedly targeting Medicare beneficiaries through deceptive telemarketing campaigns and fraudulently submitting claims to Medicare for durable medical equipment and genetic tests. As part of its takedown, DOJ announced that it is working closely with HHS-OIG, FBI, and

other agencies to create a Health Care Fraud Data Fusion Center to leverage cloud computing, artificial intelligence, and advanced analytics to identify emerging health care fraud schemes. This portends potentially even more involved prosecutions in this space.

Cyber Fraud by Health Care Companies

Recent settlements underscore the Civil Cyber-Fraud Initiative's focus on False Claims Act liability for alleged deficient or misrepresented cybersecurity in health care and federal health contracting. In July 2025, the DOJ announced that Illumina Inc. agreed to pay $9.8 million to resolve allegations under the False Claims Act arising from the company's cybersecurity practices. According to the government, Illumina made claims to federal programs and entities while allegedly misrepresenting or failing to meet certain cybersecurity requirements tied to its products and services. The settlement, in which Illumina did not admit liability, reflects DOJ's growing use of the FCA to police cybersecurity-related representations in the health care and life sciences sector.

Separately, in February 2025, Health Net Federal Services LLC and its parent, Centene Corporation, agreed to pay more than $11 million to resolve FCA allegations related to cybersecurity compliance under their TRICARE contract with the Defense Health Agency. The government alleged the companies misrepresented or failed to meet required security obligations for safeguarding sensitive health information and overseeing subcontractor compliance. Like Illumina, the matter was resolved without an admission of liability and brought under DOJ's Civil Cyber-Fraud Initiative, signaling heightened scrutiny of cybersecurity representations by federal health contractors.

This focus on health care cyber fraud is likely to be evergreen in the years ahead.

Medicare Advantage

DOJ activity in 2025 also signaled continuing focus on both civil and criminal enforcement in Medicare Advantage. In May, the United States intervened in a FCA suit against three major Medicare Advantage insurers and three large brokers alleging that the insurers paid hundreds of millions in alleged kickbacks in the form of marketing payments to steer Medicare beneficiaries into specific plans. The complaint alleges broker organizations were incentivized to sell plans based on the size of the insurers' payments and, at times, refused to sell plans from insurers that did not pay sufficient sums. The government further alleges that two of the insurers conspired with brokers to discriminate against Medicare beneficiaries with disabilities whom they perceived to be less profitable, including by threatening to withhold payments to pressure brokers to enroll fewer disabled individuals. The DOJ's decision to intervene in the case underscores the government's scrutiny of payment models tied to enrollment volume in the context of the "administrative fee" safe harbor. And as reported above, Troy Health, Inc.'s non-prosecution agreement resolved claims involving the use of AI in connection with beneficiary enrollment in Medicare Advantage plans without consent.

2025 was a busy year in and out of the courts for legal developments impacting health care fraud enforcement. These trends and decisions have broad impact both on conduct and on the crafting and company oversight of compliance programs and training. We will continue to monitor these and other subjects in 2026 and share our findings.

HIGHER EDUCATION COMPLIANCE AND GOVERNMENT ENFORCEMENT: LOOKING AHEAD TO 2026

BY MADELEINE RODRIGUEZ, EMILY NASH, HOWARD WEISS, JACE LEE, AARON LOVING, AND DEBORAH WILLIAMS

Colleges and universities have been central to the current administration's enforcement agenda, and we expect this to continue in 2026. While the focus areas for the new administration—immigration, Diversity, Equity, and Inclusion ("DEI"), and academic freedom in an era of increased protest activity—were largely expected, the tools the federal government used to enforce its policies were unconventional. The administration often pushed the boundaries of laws rarely invoked to enforce its priorities, a trend that will likely persist as we enter the next phase of the administration's plans and as responsibilities within the executive branch continue to shift.

This alert summarizes the most notable enforcement mechanisms used this past year and provides a look forward at how these tools are likely to be used in 2026.

THE DISMANTLING OF THE DEPARTMENT OF EDUCATION

In 2025, as promised, the Trump administration took a systematic approach towards dismantling the Department of Education. In March, President Trump signed an Executive Order directing the closure of the Department (the "Closure Order"), the Department announced a reduction in force ("RIF") to discharge approximately 50% of its workforce that included terminating many employees and closing the majority of the Department's offices across the nation, and President Trump announced certain programs would be transferred out of the Department. More recently, on November 18, 2025, the DOE announced six new interagency agreements with four agencies that will shift the administration of additional education programs to the Departments of Labor, Interior, Health and Human Services, and State.

Another agency taking over responsibilities shifted away from the Department is the Equal Employment Opportunity Commission (EEOC). The EEOC has played a key role in investigating university and school district policies that may violate Title VII, particularly focusing on antisemitism and anti-DEI initiatives. This includes filing a subpoena enforcement action against the University of Pennsylvania demanding that it create and disclose a list of all Jewish and Jewish-affiliated campus organizations, alongside a roster of their members, as well as lists and contact information of employees that reveal their Jewish faith or ancestry or affiliation with Jewish studies. On January 20, 2026, the university opposed the EEOC's subpoena in a forceful 163-page court filing that described the request as "an extraordinary and unconstitutional demand" that disregards "the frightening and well-documented history of governmental entities that undertook efforts to identify and assemble

information regarding persons of Jewish ancestry."

THE FALSE CLAIMS ACT AND THE DEPARTMENT OF JUSTICE'S NEW ROLE

As the Trump administration continues to dismantle the Department of Education, no agency has taken on a more significant share of increased responsibility in higher education compliance than the Department of Justice ("DOJ"). Since inauguration, the False Claims Act ("FCA") has been a central component in the administration's enforcement of its platform, especially related to issues involving civil rights.

This shift began with Executive Order 14173, "Ending Illegal Discrimination and Restoring Merit-Based Opportunity" (the "DEI Executive Order"), which forecasted that DOJ and the FCA would be heavily involved in the administration's scrutiny of higher education institutions. The Order named colleges and universities as one of the five categories for enforcement and mandated that every signatory to a funding contract certify that "it does not operate any programs promoting DEI that violate any applicable federal anti-discrimination laws." (See our previous client alert for a more in depth analysis of how this term and other aspects of the DEI Executive Order implicate the FCA.). Federal agencies have since rolled out these written certification requirements, many of which have been added to grant applications, student aid Program Participation Agreements, and other federal funding programs.

In April 2025, DOJ and the Department of Education announced a joint Title IX Special Investigations Team (the "Title IX SIT") to enforce President Trumps Executive Orders, "Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government" and "Keeping Men Out of Women's Sports." This team is likely to be active in 2026—just last week, the Title IX SIT announced an investigation into the California Community College Athletic Association based on the association's policy allowing a transgender female or non-binary student-athlete to compete on a women's team.

On May 19, 2025, DOJ also announced the launch of its Civil Rights Fraud Initiative, directing DOJ lawyers to use the FCA against federal fund recipients that violate civil rights laws. The memorandum made express reference to colleges and universities and "strongly encourage[d]" whistleblowers to file *qui tam* lawsuits under the FCA. Then, on July 29, 2025, Attorney General Bondi published a "guidance" memorandum, which outlined the administration's interpretation of federal antidiscrimination laws and provided examples (including many in the higher education space) that it viewed as "unlawful."

Such enforcement has now begun, although the administration's FCA theory and use of certifications has not yet been tested in courts. On the government-initiated side, FCA investigations by the DOJ's Civil Rights Fraud Initiative have not been made public in the higher education space, but various large public corporations—including Google and Verizon—have reportedly received subpoenas from DOJ concerning their workplace programs. Whistleblowers have also begun taking cues from the federal guidance. Recently, the District Court for the District of Columbia dismissed a plaintiff's claim against his former employer alleging that he was retaliated against for complaining of race discrimination in violation of the FCA.[1] The court found no merit to the "theory … that engaging in discriminatory conduct while conducting

a federally funded study necessarily constitutes the misuse of federal funds in violation of the False Claims Act." Notably, however, the case did not involve a certification as contemplated by the DEI Executive Order. We expect the volume of FCA investigations and lawsuits to increase this year as the framework the administration laid in 2025 begins to play out and cases are made public.

Separate from its FCA activity, DOJ has used Title VII to enforce the administration's anti-DEI stance. DOJ has authority to bring suit under Title VII against state and local governments under a 2018 memorandum of understanding between DOJ and the Equal Employment Opportunity Commission. On December 9, 2025, DOJ's Civil Rights Division brought suit against the Minneapolis Public School district alleging that a collective bargaining agreement with a teachers' union violates Title VII because it provides preferences to teachers who are members of an "underrepresented population" in employment decisions. Earlier this month, on January 14, 2026, DOJ's Civil Rights Division similarly brought suit against Minnesota alleging Minnesota violates Title VII through its statewide affirmative action program for state civil service. The Civil Rights Division is likely to continue using its authorization under Title VII to bring these types of discrimination cases. Due to the scope of the memorandum of understanding with the EEOC, these types of lawsuits will likely implicate only public universities.

As DOJ's focus on higher education has grown, the Department of Education's Office for Civil Rights (OCR)—usually a key figure in civil rights enforcement actions against higher educational institutions—has taken a back seat, as the office itself remains in limbo (for an explanation of the dismantling of the Department of Education and OCR and the corresponding legal challenges, see here). Still, while OCR's overall enforcement activity has diminished—Dissolution of the Employee Engagement Diversity Equity Inclusion Accessibility Council (EEDIAC) within OCR pursuant to President Trump's Executive Order "Ending Radical and Wasteful Government DEI Programs and Preferencing," as one example—it has not disappeared. Instead of its traditional, broader enforcement mandate, OCR's activities now closely follow the administration's priorities, including an increase in OCR-directed investigations: (1) enforcing Title VI as it applies to allegations of antisemitism arising out of Israel-Palestine protests and discrimination claims made by white individuals; and (2) enforcing Title IX in line with President Trump's Executive Order. We expect OCR to continue with this approach in 2026.

FINANCIAL AID

Financial aid is another pressure point for higher education institutions. The Department of Education has demonstrated its willingness to specifically target colleges and universities with threats to aid availability, and to deploy restrictive cash management mechanisms to induce institutional change beyond traditional means. In September, for example, Federal Student Aid placed Harvard on Heightened Cash Monitoring status and demanded a $36-million irrevocable letter of credit, citing certain "discretionary triggers," including an adverse Title VI determination. The strategy forces targeted institutions to front federal aid payments and seek reimbursement later, creating immediate cash-flow stress and operational friction even for well-capitalized institutions.

Moreover, the DEI Executive Order referenced not only colleges and universities that receive federal funding grants but also any higher education institution that participates in the federal student loan assistance program under Title IV. Of note, institutions must sign a current program participation agreement to remain eligible under Title IV and, by doing so, the institution agrees to comply with Title VI and Title IX. This is yet another tool, and yet another threat of FCA-related enforcement, that the DOJ's Civil Rights Fraud Initiative and other federal enforcement agencies could employ to target universities in 2026.

Last year also saw renewed emphasis by the Trump administration on timely repayment of student loans, with threats to institutions that do not help facilitate such payments. On May 5, Federal Student Aid published a Dear Colleague Letter noting that under Section 435 of the Higher Education Act, "institutions are required to keep their cohort default rates (CDR) low and will lose eligibility for federal student assistance, including Pell Grants and federal student loans" should their default rates become too high. As student aid and loans become increasingly important aspects of university operations, this threatens to increase both financial and administrative strains on institutions heading into 2026.

The 2026 outlook is an expansion of these and similar approaches.

ACCREDITATION

During his campaign, President Trump revealed that he would use accreditation as his "secret weapon" to enforce his educational policies. In April, President Trump issued Executive Order, "Reforming Accreditation to Strengthen Higher Education," which outlined the administration's two-pronged approach to accreditation:

- First, the Order directed the Secretary of Education to "promptly provide to accreditors any noncompliance findings related to member institutions" by OCR under Title VI or Title IX. The Department of Education has followed through on this directive, sending notices to Columbia's accreditor and Harvard's accreditor following OCR investigations.
- Second, the Order addressed a broader effort to revamp the entire accreditation system to ensure accreditors embrace the administration's priorities. The Executive Order, for example, discourages current accreditors from including "'DEI'-based standards" and directs current accreditors to require institutions to "prioritize intellectual diversity amongst faculty." The Order simultaneously encourages the creation of new accreditors. The Department of Education has pushed forward these policies. In May, the Department issued new guidance that relaxed the process for switching accreditors. Then, in November, the Department repurposed FIPSE grants to address areas aligned with the administration's policies, including "supporting institutions in changing accrediting agencies" and "supporting the creation of new accrediting agencies."

Florida and university systems in six other southern states are launching their own accrediting agency, the Commission for Public Higher Education ("CPHE"). The CPHE's business plan notes that the accreditor will be accountable to the states, which would allow state politicians to further reach into curriculum, faculty appointments, and every aspect of the public institution's operations.

Accreditation is a powerful tool: If a school loses accreditation, students at those schools lose eligibility for federal financial aid. Even informal signals that accreditation could be jeopardized could affect students' willingness to risk enrolling at an institution. With enrollment pressures already reaching new highs, accreditation threats seem poised to exert substantial pressure on institutions.

FEDERAL FUNDING AS A CARROT AND A STICK

Grant terminations have been a hallmark of the Trump administration's enforcement strategy. Last year saw a flurry of efforts by the government to freeze or cancel funding to colleges and universities. Some universities challenged the federal grant freezes, and have been successful (see here for a discussion of these cases), but many negotiated resolutions that restored funding in exchange for payments and policy commitments.[2]

With the reliability of existing federal funding now on shakier ground, the administration has also began wielding grant funding as an incentive to accept its proposals. On October 1, 2025, the White House sent letters to nine universities promising preferential federal funding to those who signed a "Compact for Academic Excellence in Higher Education." This Compact includes a variety of requirements aligned with the administration's priorities—from "revising governance structures …, including but not limited to transforming or abolishing institutional units that purposefully punish, belittle, and even spark violence against conservative ideas" to "defining and otherwise interpreting 'male,' 'female,' 'woman,' and 'man' according to reproductive function and biological processes." After a lukewarm response from the original nine universities, President Trump later announced that any college would be eligible to receive preferential federal funding if they signed the Compact. To date, the New College of Florida has been the only school that publicly stated its intent to sign the Compact.

Heading into 2026, the Department of Education is poised to continue vigorously pursuing and enforcing resolution agreements that tie grant eligibility to institutional policy changes. While the administration may continue the across-the-board freezes it began in 2025, it may also refine its approach in light of the court rulings in California and Massachusetts, building fuller administrative records, targeting more specific funding programs on more specific bases, and employing other moderating tactics to withstand potential judicial review. The likely result is more durable funding freezes or terminations designed to encourage favorable settlements and overcome litigation challenges as the administration continues to watch for institutional policies and practices contrary to its goals.

PUBLIC INSTITUTIONS AND PRESIDENTS

In another unconventional approach, the Trump administration engaged in several public initiatives to force university leadership change. Public institutions were especially vulnerable to this type of attack, and two such institutions—the University of Virginia ("UVA") and George Mason University ("GMU")—illustrate the strategy.

UVA President Jim Ryan resigned in June 2025 following sustained political pressure to do so. On March 7, 2025, the Board of Visitors—responsible for the long-term planning of the university—

passed a resolution to dissolve the university's Office of Diversity, Equity, Inclusion and Community Partnerships, relying on the Trump administration's interpretation of the Equal Protection Clause, Title VI, and other federal civil rights laws. Then, DOJ began putting pressure on UVA, often specifically focusing on Ryan. In April, after UVA received two letters from DOJ inquiring into the university's use of race in its admissions policies, DOJ sent a third letter directly addressed to Ryan referencing complaints that he was failing to implement the Board's resolution. In May and June, DOJ sent four additional letters about opening a Title VI investigation into the school related to allegations of antisemitism. The last letter specifically threatened the "suspension, termination, or refusal to grant or continue UVA's federal financial assistance." Behind the scenes, Gregory Brown, the deputy assistant attorney general for civil rights, reportedly demanded Ryan's resignation. Ryan ultimately announced his resignation on June 27, 2025. With new leadership in place, UVA announced an agreement with DOJ that it would "be bound by the Department of Justice's 'Guidance for Recipients of Federal Funding Regarding Unlawful Discrimination.'"

GMU President Gregory Washington was the next university leader in the administration's crosshairs. In the span of just a few weeks in July, OCR and DOJ opened four civil rights investigations examining whether GMU's hiring and admissions practices violate federal nondiscrimination laws. On August 22, 2025, the Department of Education announced that it determined GMU violated Title VI and issued a proposed Resolution Agreement. The announcement specifically targeted Washington, noting that "under his leadership and direction, the University violated Title VI by illegally using race and other immutable characteristics in university practices and policies, including hiring and promotion," and demanded the president issue a "personal apology." Washington refused. Since then, members of the House Judiciary Committee have publicly accused President Washington of making misleading or false statements to Congress regarding the scope and operation of GMU's DEI programs and compliance practices. This fight for control of the university continues into 2026.

The government can assert meaningful influence by targeting leadership at institutions viewed as resistant or misaligned, without resorting to legislation or litigation. If 2025 served as a testing ground, 2026 is likely to see more individualized interventions, as governments increasingly seek to shape public institutions through the people who lead them.

GOVERNMENT'S PARTNERSHIP WITH STATES TO INFLUENCE CURRICULUM AND INSTITUTIONAL OPERATIONS

In 2025, the federal government increasingly worked in concert with states to influence—and often succeeded in influencing—how schools operate, what they teach, and how they hire. These efforts have reached public and private universities alike.

Florida, through Senate Bill 266, enacted legislation dictating how state colleges and universities may allocate funds, structure hiring processes, and frame academic offerings related to DEI—including by barring public universities from offering courses based on theories of systemic racism and sexism. Ohio Senate Bill 1, among other things, sets rules around classroom discussion surrounding diversity-related topics and prohibits any new institutional scholarships that "use

diversity, equity, and inclusion in any manner." And Texas A&M's Board of Regents—individuals appointed by the governor—approved a policy stating that "no system academic course will advocate race or gender ideology, or topics related to sexual orientation or gender identity," with a narrow exception for certain non-core curriculum or graduate courses (that still must be reviewed and approved by the campus president). In Oklahoma, state education officials have sought to exert control over classroom content and staffing by adopting controversial social-studies standards and new credentialing requirements for teachers. In August 2025, Oklahoma announced that out-of-state teachers from jurisdictions such as California and New York would be required to pass an "assessment exam" as a condition of licensure, a measure state officials explicitly described as a way to safeguard against "radical leftist ideology."

Florida's experience also illustrates how legislation can be paired with governance restructuring to produce more targeted outcomes. In 2023, Florida Governor Ronald Desantis effected what was called a "hostile takeover" of the New College of Florida, previously known as a progressive school, by replacing key trustees, shifting control of the board, and enabling rapid changes to leadership at the school. Governor Desantis was able to establish his academic priorities within the school—the new president of the school, Richard Corcoran, was Governor Desantis's first Commissioner of Education. Demonstrating the school's changed priorities, New College was the first to say it would sign the Trump administration's Compact for Academic Excellence in Higher Education, which links preferential access to federal funding to a willingness to adhere to a set of conditions aligned with the administration's educational goals. Now, Governor Desantis intends to expand New College's footprint and his control over state universities by proposing a transfer of the University of South Florida Sarasota-Manatee's campus to New College. Curriculum, appointment of university leadership, and faculty hiring decisions—all realms that used to be protected from government control—have now become vulnerable to governmental intrusion, and we expect federal and state actors to continue working together to insert themselves into higher educational institutions' operations in 2026.

***

In sum, the Administration is highly motivated to enforce its policy priorities and is using all of the tools at its disposal to do so. Most recently, the Department of Education used the Jeanne Clery Campus Safety Act ("Clery Act")—which generally requires any institution participating in federal student aid programs to collect, classify, and disclose campus crime statistics and safety information—to target certain universities. In November and December, the Department of Education publicly announced Clery program reviews at the University of California, Berkeley following a protest at an event organized by Turning Point USA, and at Brown following a campus shooting. The administration also used Section 117 of the Higher Education Act, a law requiring institutions receiving federal aid to submit disclosure reports on foreign gifts and contracts valued at $250,000 or higher to the Department of Education, to investigate universities. Investigations were announced as to the University of California, Berkeley, Harvard, and the University of Pennsylvania.

Whether these are isolated incidents or tools that the administration will seek to use more in 2026 broadly remains to be seen, but it is indicative that nothing is off the table. Any compliance

requirement for colleges and universities may be exploited, and higher education institutions' operations will remain highly scrutinized in 2026.

---

[1] Thornton v. NAS, No. 25-cv-2155, 2025 U.S. Dist. LEXIS 220605, at *5, 7 (D.D.C. Nov. 7, 2025).

[2] For example, after funding freezes tied to antisemitism and other civil rights allegations, Columbia University settled with the Department of Education, DOJ, and Department of Health and Human Services ("HHS") in late July for $221 million and acceptance of a variety of terms, in exchange for restoration of over $400 million in federal grants. Columbia agreed to, among other things, (i) provide the federal government access to data and information about its hiring, admissions, and university programming to assess its compliance with the administration's interpretation of federal civil rights laws; (ii) "a comprehensive review of [its] portfolio of programs in regional areas, starting with those relating to the Middle East"; and (iii) "foster[] new faculty appointments to promote intellectual diversity." Columbia also agreed to have an independent Resolution Monitor and an Administrator oversee these operational changes. Brown University likewise reached an agreement restoring funding from the HHS in exchange for a commitment of $50 million to Rhode Island workforce development organizations and compliance with federal priorities concerning antisemitism, gender policy, and admissions. Agreements with Cornell University, Northwestern University, and the University of Pennsylvania followed the same general pattern.

ANTICORRUPTION ENFORCEMENT AND THE FCPA: 2026 YEAR IN PREVIEW

BY ADAM SAFWAT, ANTHONY D. MIRENDA, DANIEL ZALEZNIK AND JOSHUA NACHT

2025 saw fundamental shifts in Foreign Corrupt Practices Act (FCPA) enforcement priorities under the first year of the second Trump Administration. FCPA and global anti-corruption landscape enters 2026 amid continued recalibration in U.S. enforcement priorities, a thinned but active federal enforcement apparatus, and increasingly assertive international counterparts filling perceived gaps left by shifting U.S. policy.

U.S. ENFORCEMENT BACKDROP AND POLICY DIRECTION

The defining story of 2025 was the White House–directed "pause" in new criminal FCPA casesand a subsequent DOJ review that closed some matters, allowed others to proceed, culminating in the June 2025 Guidelines for Investigations and Enforcement of the FCPA (2025 FCPA Guidelines) issued by Deputy Attorney General Todd Blanche. Those Guidelines steer prosecutors toward cases that vindicate U.S. interests—corruption cases involving international drug cartels and Transnational Criminal Organizations (TCOs), harm to identifiable U.S. competitors, and matters implicating national security sectors, such as corruption in the defense sector. The 2025 FCPA Guidelines also emphasize DOJ's interest in pursuing matters showing strong indicia of corrupt intent rather than low-dollar matters involving common business courtesies. DAG Blanche reiterated at the December 2025 ACI FCPA Conference that enforcement "is not slowing down," but will be disciplined, trial-ready, and centered on conduct that "matters to the American people." DOJ has also signaled it will not stretch the FCPA to reach conduct involving marginal U.S. connections, with deference to foreign authorities where appropriate.

The new FCPA Guidelines will be applied in tandem with DOJ's new guidance on corporate enforcement, issued in May 2025, which includes new guidance on crediting voluntary disclosures to encourage companies to self-report. The Criminal Division's updated Corporate Enforcement and Voluntary Self-Disclosure Policy (CEP) provides a declination when a company (1) voluntarily self-discloses to the Criminal Division, (2) fully cooperates, (3) timely and appropriately remediates, and (4) there are no aggravating circumstances related to the offense. Prosecutors may still recommend a declination in their discretion even if aggravating factors exist, but any declination will require payment of disgorgement and restitution and will be made public. When a company either made a good faith report that does not technically qualify as a voluntary self disclosure because DOJ was already aware of the criminal activity or the conduct has aggravating factors that warrant a resolution, DOJ may still offer a non prosecution agreement (NPA) that will allow a

term under three years, will not require a monitor, and will grant a 75% reduction off the low end of the U.S. Sentencing Guidelines (USSG) fine range. In other cases where these options are not available, prosecutors retain discretion on form, term, and compliance obligations, but any monetary penalty reduction will be capped at 50% off the USSG fine. The starting point in the Guidelines range may vary based on case-specific facts, including recidivism. This additional guidance regarding credit even for partial or imperfect disclosures is intended to encourage disclosures, but it underscores that any disclosure decision requires many factors to be considered.

We will watch to see, in 2026, how DOJ's application of its new FCPA Guidelines plays out in terms of the type and number of new cases charged and investigations opened.

In late 2025, DAG Blanche articulated five charging principles that will also affect FCPA cases: (1) individual accountability; (2) charging only where admissible evidence supports guilt beyond a reasonable doubt (3) rewarding cooperation; (4) streamlining investigations; and (5) orderly internal elevation. DOJ has previewed a department-wide corporate enforcement policy to harmonize incentives and expectations across components, which should further codify the 2025 shifts.

Monitorships are being recalibrated to limit their scope to address the issues at the heart of the underlying matter. The Administration also seeks to lower the costs associated with previously expansive monitorships. Under new guidelines issued in May 2025, DOJ will review existing monitors to ensure they meet the Department's new narrowly tailored approach. DOJ will also impose budget and fee caps requirements for new monitorships, aiming to keep costs proportionate to the severity of the underlying conduct, the profits of the culpable entity, and the scale of the organization. In parallel, DOJ's May 2025 white-collar enforcement memorandum set criteria for early termination of post-resolution reporting obligations, emphasizing progress, risk reduction, and remediation maturity—considerations that will influence corporate strategy in 2026. Shortly before the onset of the new guidelines, DOJ terminated the monitorship of Glencore, which stemmed from FCPA violations, three months early. Later in the year, DOJ reportedly terminated another corporate monitorship over 15 months early.

ENFORCEMENT THEMES FOR 2026

DOJ's FCPA work will continue to prioritize cases with meaningful U.S. touchpoints while aligning with broader white-collar priorities in trade fraud, sanctions/money laundering, and integrity of U.S. markets. The 2025 guidance explicitly targets conduct intertwined with cartels and TCOs; companies with supply chain exposure in high-risk corridors—particularly those with unavoidable "touchpoints" to cartels—should expect intensifying diligence expectations and investigative interest. At the same time, DOJ messaging underscores restraint against over-criminalizing de minimis business courtesies, focusing resources on provable, high-impact schemes.

Beyond classic bribery patterns, practitioners should monitor adjacent 2026 risk areas that can intersect with foreign bribery investigations: trade and tariff evasion schemes, government contract fraud, and misuse of digital assets for sanctions evasion or payments laundering.

THE ENFORCEMENT CADENCE AND THE SEC

After a near four-month silence during the pause, DOJ returned to a more "traditional cadence" in late 2025, with the FCPA Unit previewing a mix of corporate and individual matters to be announced in 2026. Even so, staffing remains lean—roughly a dozen prosecutors at DOJ's FCPA Unit—and SEC's specialized FCPA Unit appears to have been effectively dissolved, with no SEC FCPA actions publicly observed in 2025 and former leadership departed. To date, under the current administration, there have been no foreign bribery resolutions announced by the SEC. This may be reflective of the administration's intent to turn away from charging some of the lower-dollar business courtesies cases that were often charged by the SEC as books and records violations.

CASE GENERATION AND WHISTLEBLOWERS

Case intake should remain robust in 2026 from voluntary self-disclosures, a stepped-up whistleblower pipeline, and interagency referrals. DOJ reports that is has received more than 1,100 submissions under the Criminal Division's Whistleblower Awards Pilot Program since its launch in 2024. As originally launched, the program included referrals for FCPA cases. In 2025, DOJ expanded the scope of this program to include referrals involving trade and customs fraud and international criminal cartel activity. Given that these areas have the possibility to overlap with international corruption matters, we will look to see whether the expanded scope of the program will generate new FCPA leads and investigations.

DOCTRINAL DEVELOPMENTS

There were meaningful developments in FCPA jurisprudence in 2025:

- ***U.S. v. Ng Chong Hwa,* 161 F.4th 127 (2d Cir. 2025).** The Second Circuit affirmed the conviction of Goldman Sachs Director Roger Ng under the FCPA in a bribery scheme related to 1 Malaysian Development Bank (1MDB). The court confirmed a broad venue holding, with conspiracy-related telecommunications and travel sufficient to permit venue in EDNY.
- ***U.S. v. Leissner,* 18-CR-439 (MKB), 2025 U.S. Dist. LEXIS 102348 (E.D.N.Y. May 29, 2025).** In another 1MDB case, the district court denied restitution to a third party following the Defendant's guilty plea on FCPA-related charges. The victim purported to suffer political recriminations after sharing information leading to FCPA enforcement. The court held that the victim was not entitled to restitution because his harms were not tied directly to the crimes of conviction, narrowing available restitution for FCPA violations under the Mandatory Victims Restitution Act.
- ***U.S. v. Oztemel*, 23-cv-00026 (KAD), 2025 U.S. Dist. LEXIS 154283 (D. Conn. Aug. 11, 2025).** A court rejected a defendant's post-conviction challenge to jury instructions that implied that the defendant could be simultaneously an "agent of domestic concern" under section (a)(1) and a "person" under section (a)(3), holding that the Government was not required to elect at trial on which sub-section of the FCPA the defendant was charged.

- ***Rycar Tr. v. Yates Fam. Invs.,* 23-CV_00732-TC-DAO, 2025 U.S. Dist. LEXIS 177853 (D. Utah Sept. 8, 2025).** In granting a motion to dismiss a securities fraud lawsuit, the district court held that there is generally no duty to disclose uncharged FCPA investigations.

2025 DOJ ENFORCEMENT ALIGNS WITH NEW FCPA PRIORITIES, SIGNALING THE SAME FOR 2026

Several 2025 matters set up inflection points in 2026. The indictment of Smartmatic, the voting machine company, was the first the first corporate FCPA indictment in 15 years—added to preexisting individual charges tied to alleged bribes in the Philippines—and foreshadows a contested corporate case with political overtones. The superseding indictment alleges an over-invoicing slush fund, encoded communications, and laundering through accounts in Asia, Europe, and the United States, with multiple individual defendants and fugitives. We expect that Smartmatic may make pretrial motions that may raise issues regarding jurisdiction and extraterritoriality, among other issues.

In November 2025, DOJ announced that it had entered into a two-year Deferred Prosecution Agreement (DPA) with TIGO Guatemala, a cellular network provider, in the Southern District of Florida—resulting in over $118 million in combined criminal penalty and forfeiture. The DPA resulted after DOJ re-opened its investigation into TIGO in 2020 with the emergence of new evidence that criminal conduct continued after the Department initially closed the investigation in 2018. The DPA describes a long-running cash-for-votes scheme aimed at Guatemalan legislators, with some payments funded by narcotrafficking proceeds, an area of high priority enforcement under the new FCPA Guidelines. In 2026, we will see whether the case signals DOJ's readiness to charge corporations under the FCPA when the underlying corruption allegations relate to its new high priority areas.

Additionally, the December 2025 Houston jury conviction of a Texas-based executive for bribing officials at a foreign state-owned oil company underscores DOJ's willingness to try individual FCPA cases to verdict. The evidence showed six-figure bribe payments and luxury items exchanged for contract advantages worth millions. The indictment was brought in August, only four months before the case went to trial. The speed at which the case progressed demonstrates DOJ's serious commitment to efficient FCPA prosecutions under the new guidelines. In 2026, we will look to see how DOJ uses the new FCPA Guidelines in making charging decisions against individuals.

COMPLIANCE IMPLICATIONS FOR 2026

For multinational companies, 2026 planning should assume an active but more selective U.S. enforcement environment that rewards speed, proof, and tangible remediation while intensifying scrutiny of high-risk third parties, distributors, and logistics nodes with potential TCO and cartel interfaces. The practical consequences are clear: fortify third-party risk management and supply chain diligence; document investigative steps and remediation contemporaneously; be prepared for compressed timelines; and align incident response to support timely voluntary disclosures where warranted, particularly when the corporation can demonstrate it had implemented a robust

compliance program and is prepared to provide evidence regarding problematic individual conduct to authorities.

Finally, even if the SEC's inactivity in FCPA enforcement continues (and we cannot predict that it will), private securities and derivative shareholder litigation remain active FCPA risks. In particular, companies should note that derivate shareholder litigation aimed at a public company board's supervision of the scope and effectiveness of company compliance programs remains a risk for those companies that do not have a robust FCPA compliance program.

GLOBAL DEVELOPMENTS

In reaction to apparent US pullback from global anti-corruption efforts, international organizations took steps to fill the void. On March 20, 2025, the UK's Serious Fraud Office, together with the Swiss Office of the Attorney General ("OAG") and the French National Financial Prosecutor (*Parquet National Financier,* "PNF") announced the creation of an International Anti-Corruption Prosecutorial Taskforce. The taskforce's mandate provides for exchange of information and coordination of strategy on cases between the cooperating countries' enforcement authorities, while fostering cooperation and future operational collaboration.

In light of the Trump Administration "pause" on FCPA enforcement, and prior to the issuance of the June 2025 Guidelines, DOJ notably did not participate in the OECD Working Group on Bribery in March of last year, prompting concerns about future participation in the Anti-Bribery Convention. DOJ attended the OECD meeting in June, providing an update on developments including the issuance of the FCPA Guidelines and reaffirming the U.S. commitment to prosecuting foreign bribery. The OECD working group invited the U.S. to provide a written update in December 2025. That report remains pending.

Separately, the World Bank has continued to be active in enforcing sanctions on entities engaged in corrupt practices, which include fraud or corruption as related to Word Bank Group-financed projects. In 2025, the World Bank undertook at least twelve enforcement actions, including sanctions, debarment, or settlement agreements with individuals or entities engaged in such actions. Most recently, on December 11, 2025, the Bank announced a 24-month sanction of Turkish based Teknoloji Enerji Ve Muhendisilk A.S. for fabricating performance reporting documents and impeding the subsequent investigation.

KEY TAKEAWAYS

- 2026 will likely feature disciplined FCPA enforcement keyed to U.S. interests, with a premium on trial-ready cases, individual accountability, and demonstrable cooperation and remediation.
- Expect heightened attention to supply chains intersecting with TCOs, cartels, adjacent trade fraud and money flows, and public-procurement touchpoints—especially in higher-risk geographies.

- International authorities are coordinating more closely and sharpening tools, which will sustain global enforcement pressure even if U.S. volumes fluctuate.
- Companies that invest early in risk-based controls, swift investigations, and voluntarily proffer evidence of wrongdoing by individuals, where applicable, will be best positioned for declinations, credit, or streamlined resolutions.

SECURITIES ENFORCEMENT AND REGULATORY DEVELOPMENTS FROM THE SEC, CFTC, AND PCAOB

BY ANTHONY D. MIRENDA, ADAM SAFWAT, MATTHEW E. MILLER, LEAH S. RIZKALLAH, RACHEL KERNER, GILLEUN KANG, MARILYN ICSMAN AND JOSHUA NACHT

2025 saw fundamental shifts in securities enforcement priorities in the first year of the second Trump Administration. The SEC and the financial regulatory landscape enters 2026 amid continued refocusing of policy priorities: a recalibration of regulatory actions surrounding compliance issues and ESG financial statement disclosures; a harmonized approach to cryptocurrency that differentiates between securitized and non-securitized digital assets and seeks to promote digitalization of other traditional securities; a revamp of the Wells Process; and continued emphasis on individual accountability; and as continued adjustment of administrative enforcement adjudication stemming from the Supreme Court's 2024 *Jarkesy* decision. Despite these new initiatives, recent enforcement actions under the new SEC leadership underscore that traditional fraud enforcement, including financial statement fraud, will continue to be a priority for the SEC in 2026.

THE BIG PICTURE

a. Enforcement in Traditional Fraud Areas Continues

Following Chair Gary Gensler's departure in January 2025, Commissioner Mark Uyeda stepped in as Acting Chair until Chair Paul Atkins was sworn in on April 21, 2025. Commissioner Uyeda was a vocal critic of the SEC's regulatory enforcement sweeps surrounding record keeping and of new proposed rules requiring ESG disclosures and began the shift in the SEC's current approach away from Chairman Gensler's more aggressive regulatory approach. Chair Atkins, for his part, spoke out against the prior administration's pursuit of large corporate fines and enforcement actions that "consume excessive Commission resources not commensurate with any measure of investor harm." Thus, under new leadership, the SEC signaled a return to bread-and-butter enforcement, focusing on fraud that directly harms investors, prioritizing insider trading, offering fraud, Ponzi schemes, market manipulation, and adviser fiduciary breaches over more novel or technical violations. The Commission's 2025 enforcement data reflects this "back to basics" approach: of at least 91 new enforcement suits filed from inauguration through September, nearly 33% targeted offering fraud or insider trading.

Illustrative actions underscore this trajectory. Throughout 2025, the SEC initiated actions against various individuals and companies for operating multi-million-dollar Ponzi schemes and defrauding investors. The Commission also charged individuals in an international insider trading ring that allegedly reaped about $17.5 million using coded and disappearing messages, with parallel criminal indictments unsealed in Massachusetts. These examples suggest that, looking forward into 2026, we can expect a

continued emphasis on traditional fraud focusing on investor harm and a renewed attention to insider trading, accounting fraud, offering fraud and Ponzi schemes.

b. Moving Away From Regulation By Enforcement While Promoting Market Integrity

Under the SEC's new leadership, we expect a recalibration in enforcement priorities for companies: while the SEC continues to probe potential violations of accounting and auditing standards, companies should anticipate less emphasis on technical or minor violations, and more focus on clear-cut violations that amount to fraud or mislead investors. Chair Atkins has also signaled a commitment to provide businesses notice of technical violations before enforcement action. As he put it in a recent interview, the SEC is moving away from a "shoot first, ask questions later" approach and will not be "bashing down [a company's] door" over technical missteps without warning. The SEC also voted to end its defense of rules requiring disclosure of climate-related risks and greenhouse gas emissions, with Chairman Uyeda calling those rules "costly and unnecessarily intrusive."

While enforcement actions related to earnings management have also declined in 2025, following several years of increased enforcement activity in this area due to the SEC's "EPS Initiative" (which applied data analytics to review financial disclosures for evidence of manipulation), the current SEC's approach remains unclear and we will watch how the SEC pursues earnings management cases in 2026.

However, the SEC's recalibration with respect to financial statement oversight does not mean that it is abandoning its traditional role of scrutinizing public companies' disclosures about their financial performance. On January 27, 2026, the SEC announced settled charges against a major public company and several of its former executives for materially inflating the performance of a key business unit by using accounting techniques to transfer operating profit from other business units to the underperforming unit. Although the SEC credited the company for its cooperation and remediation, it was still required to pay a civil penalty of $40 million, and its former executives also had to pay civil penalties and disgorgement—in one case, over $600,000 in total fines. The SEC's new Director of Enforcement, Margaret Ryan, touted this case as an example of the SEC stepping in to maintain "market integrity" for investors.

The takeaway is not that enforcement is softening across the board; rather, it is becoming more targeted. Indeed, the retreat from a more aggressive regulatory strategy may result in a shift of resources toward more classic financial statement cases, resulting in a potential uptick in such cases in 2026. Cases most likely to be brought in 2026 will likely feature clear deception, concrete investor impact, or straightforward breaches of accounting and auditing standards.

c. The Investment Services Industry Should Remain Vigilant

One of the most immediate and notable shifts under acting Chair Uyeda and Chair Atkins has been the move away from enforcement sweeps pursuing regulatory violations. Under the prior administration, the SEC conducted sweeps of the investment industry targeting violations of record keeping requirements. Alongside sweeps for violations of the SEC's Marketing Rule concerning unsubstantiated fund performance claims in advertising, these broad enforcement actions resulted in significant penalties. Chair

Atkins has made it clear, however, that the Commission will move away from these enforcement sweeps that "consume[] excessive Commission resources not commensurate with any measure of investor harm."

This shift in focus should not be confused with a laissez faire approach to the investment services industry. Enforcement actions in the latter part of 2025 after Chair Atkins assumed his position in April signal that in 2026, the SEC will focus on investigating insider trading under classic theories of breach of trust and fiduciary duties and misappropriation of material nonpublic information (MNPI). For example, in September 2025, the SEC filed charges against an equity trader for trading on MNPI that he acquired from his firm about secondary public offerings. The SEC pursued a classic theory against the trader of breaching his duty of trust to his employer by misusing confidential information. On January 29, 2026, the court entered final judgment permanently enjoining the defendant from violating the Securities Acts and imposing a civil penalty and disgorgement plus prejudgment interest. *See SEC v. Squillante*, No. 3:25-cv-01457-SFR (D. Conn. filed Sept. 5, 2025). In another case also filed in August, the SEC charged a former investment relations manager for tipping his friends with MNPI about public biotechnology companies. The tippees who profited on trading on the information were also charged, and the court entered final judgment permanently enjoining them from violating the charged provisions and authorizing the court to determine at a later date the amount of disgorgement, prejudgment interest, and civil money penalties that each defendant shall pay. *See SEC v. Yedid et al.*, No. 1:25-cv-06704 (S.D.N.Y. filed Aug. 18, 2025).

In a similar vein, the SEC continues to scrutinize investment advisors who become privy to information about an offering but short sell during the restricted period ahead of the offering in violation of Rule 1-5 of Regulation M.

In addition, we expect that in 2026, the SEC will continue the approach of previous administrations of scrutinizing practices of investment advisors that result in hidden costs and fees. Last year, the SEC investigated advisors for conflicts of interest related to undisclosed fees. In August 2025, the SEC charged two investment advisors for failing to disclose fees and incentives in connection with fee-based investment services.

d. Increased Focus on Individual Accountability

Since taking office, Chair Atkins has signaled a shift toward individual accountability for securities violations, believing that penalties targeting culpable individuals provide the needed deterrent impact (perhaps even more effectively) without imposing collateral damage on shareholders. Whether a focus on individual accountability will actually result in a shift away from significant corporate penalties remains to be seen. Of note, the resolution listed above for financial statement manipulation against a public company—which included significant penalties against its former executives—also included a $40 million civil penalty against the company.

HOT TRENDS AND CASES FOR 2026

a. Crypto-Policy: From "Regulation-by-Enforcement" to "Project Crypto" and a Coherent Token Taxonomy

In 2026, the SEC continues its shift from enforcement-led boundary setting to rulemaking, exemptive relief, and interagency policy-anchored by Chairman Atkins's "Project Crypto" and a formal "token taxonomy." In 2025, the SEC closed or dismissed high-profile crypto matters for policy reasons, signaling that

guardrails will come from guidance and notice-and-comment, not through enforcement actions. That reset alongside the newly-launched Crypto Task Force, designed to introduce regulatory and enforcement clarity, establishes 2026 initiatives to review cryptocurrency distributions, custody, trading, and the classification of tokenized securities.

At the center of the SEC's new approach is "Project Crypto." The plan harmonizes oversight and regulation of digital assets, in order to provide clear guidance on classifying various assets (such as stocks and bonds that trade like other crypto assets on blockchain), to differentiate between non-securitized and securitized digital assets, and to promote the distribution of earnings in digital asset securities. Chairman Atkins instructed staff to allow exemptions during rulemaking, including proposals to let "super-apps" operate under a single license and to allow SEC registrants to list non-security crypto assets alongside traditional securities.

A planned "token taxonomy" underlies the new policy. Chairman Atkins previewed a framework that treats most tokens as not inherently securities, though some distributions can be investment contracts under the traditional Howey test. *SEC v. W.J. Howey Co.*, 328 U.S. 293, 298-99 (1946). The taxonomy would distinguish "digital commodities" or "network tokens," "digital collectibles," "digital tools," and "tokenized securities," with only the last category considered securities as representations of traditional financial instruments in blockchain. The framework recognizes that investment contracts can end; secondary trading of non-security tokens is not per se a securities transaction once issuer promises lapse.

Interagency coordination on crypto assets will continue to increase in 2026. The SEC and CFTC issued joint statements on spot crypto (i.e., crypto assets that are bought and sold at their current market prices) and aim to reduce red tape by enabling portfolios with SEC and CFTC-regulated holdings to avoid duplicative compliance filings with both agencies. SEC staff are designing disclosure regimes, exemptions, and safe harbors for various crypto ventures to smooth the path for digital token traders to operate in the U.S. under a clear regulatory backdrop. Together with the taxonomy, these steps aim to reshore capital formation and provide bright-line tests for when assets are securities and when they involve an investment contract.

According to a speech by Chair Atkins on the digital finance revolution, Project Crypto is expected to bear the following fruit in 2026. First, a proposal or policy statement crystallizing the token taxonomy, with clear examples demarcating the boundaries between digital tokens treated as commodities and those regulated as securities. Second, updated guidelines for financial advisers regarding best practices for safekeeping clients' crypto assets ("custody rule modernization"), building on the 2025 state trust company no-action letter. Third, rules or exemptions enabling "super-apps" and side-by-side trading of non-securities and crypto asset securities on SEC-regulated platforms, plus pathways for tokens tied to investment contracts to trade on non-securities platforms under appropriate oversight. Each aims to replace ad hoc enforcement with durable market-structure rules that can keep lawful innovation onshore.

b. FCPA

In June 2025, the Department of Justice issued guidelines for the prosecution of new investigations and cases under the Foreign

Corrupt Practices Act ("FCPA"). The guidance explicitly noted a shift away from FCPA cases based on lower-value business courtesies. Previously, the SEC had pursued such cases as books and records violations under the FCPA. In 2025, however, the SEC did not initiate any new FCPA enforcement actions and its senior FCPA leadership departed. The SEC's approach to the FCPA in 2026 remains uncertain. A more detailed discussion of what to expect in 2026 regarding anticorruption enforcement and the FCPA can be found here.

c. Disgorgement

As 2026 unfolds, we are closely following how the Supreme Court will define the contours of the SEC's disgorgement authority. In 2025, federal appellate courts further split over what the SEC must prove to obtain an award of disgorgement as a remedy, which the SEC typically seeks in civil enforcement actions to return "ill-gotten gains" from securities laws violations. The Supreme Court has previously recognized that disgorgement functions as a penalty and is thus subject to a five-year statute of limitations, *see Kokesh v. SEC*, 581 U.S. 455 (2017), and instructed that the SEC could obtain disgorgement as "equitable relief" only if it does not exceed the wrongdoer's net profits and disgorged funds are returned to victims, *see Liu v. SEC*, 591 U.S. 71 (2020).

The current circuit-split centers on whether the SEC must prove investor pecuniary harm to obtain disgorgement under 15 U.S.C. § 78u(d)(5) and (d)(7), a question the Supreme Court agreed to decide in *Sripetch v. SEC* this term. In *Sriptech*, the Ninth Circuit agreed with the First Circuit's holding in Navellier that the SEC was not required to prove investors suffered a monetary loss to obtain disgorgement. *SEC v. Sripetch*, 154 F.4th 980 (9th Cir. 2025), *cert granted Sripetch v. SEC*, No. 25-466, 2026 LX 33103 (Jan. 9, 2026); *SEC v. Navellier & Assocs., Inc.*, 108 F.4th 19, 41 (1st Cir. 2024). The Second Circuit has held, however, that the SEC must prove that investors suffered monetary loss before disgorgement is available. *SEC v. Govil* 86 F.4th 89, 106 (2d Cir. 2023).

The petitioner in *Sripetch* asked the Supreme Court to resolve the split, highlighting the nationwide consequences. The SEC urged review as well and defended a profits-focused understanding that does not require investor loss. In the Supreme Court, the question presented is whether a showing of investor pecuniary harm is a prerequisite to disgorgement in SEC civil actions, potentially setting up a decision that could impact the SEC's enforcement strategies moving forward.

d. Wells Process

The coming year will put in practice the SEC's revamped approach to the Wells process, which Chair Atkins has framed as an essential extension of due process rather than a bureaucratic hurdle, with reforms intended to deliver more time, transparency, and meaningful engagement before the Commission decides whether to pursue an enforcement action. The Wells process is the mechanism by which respondents are informed of the charges the Enforcement Division Staff intend to recommend to the Commission. Respondents then have an opportunity to provide their position on why charges should not be pursued before the Commission makes a final enforcement decision. The changes discussed below reposition Wells practice as a consequential advocacy stage.

Enforcement Staff must provide at least four weeks for respondence to submit Wells submissions after being notified of intended charges by the Staff—formally moving the

baseline beyond the commonly used two-week timetable. The Staff must be "realistic" about timing in light of case complexity and are expected to grant reasonable extensions where appropriate. Staff are also directed to provide greater access to the evidentiary basis for the contemplated charges, including the investigative file consisting of transcripts and key documents—a practice often described as a "reverse proffer"—subject to statutory and programmatic confidentiality limits. These procedural safeguards are designed to sharpen the issues, improve accuracy, and ensure the Commission benefits from adversarial testing before it acts.

The Commission has also restored the direct review of all Wells submissions by the Commissioners in both settled and litigated matters, reversing prior practices that sometimes filtered or limited what reached the Commission. In addition, senior Enforcement Division leadership has been directed to meet with defense counsel prior to making recommendations. In parallel, Chair Atkins endorsed the use of pre-Wells "white papers," which allow parties to address factual or legal issues pivotal to the investigation earlier, potentially obviating a Wells notice. Under the refined framework, these white papers will also be reviewed by the Commissioners.

These Wells reforms operate alongside a broader organizational centralization within the Division of Enforcement—replacing Regional Directors with Deputy Directors and consolidating oversight—which is intended to produce greater consistency across SEC offices.

Practically, we expect respondents to make more robust use of the expanded record access and additional time to craft targeted submissions that address factual gaps, legal infirmities, and policy considerations. We also anticipate wider deployment of white papers in matters where early correction of the Staff's working theory could avoid unnecessary investigative costs.

e. Shadow Trading Theory

Enforcement of "shadow trading" has been a hot topic since the SEC advanced the theory in 2024 in *SEC v. Panuwat*, and 2026 is expected to finally bring some clarity to the SEC's view of its scope and application. Shadow trading is a novel insider trading theory in which a person with material non public information about Company A trades in the securities of Company B—a competitor or comparable company whose value is likely to be affected. In *Panuwat*, the SEC alleged that Panuwat, 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 announcement that Pfizer would acquire Medivation at a significant premium. According to the complaint, Panuwat knew that investment bankers had cited Incyte as a comparable company in discussions with Medivation and anticipated that the Medivation acquisition would likely lift Incyte's stock price.

In April 2024, Panuwat was found liable for insider trading under the shadow trading theory. The case was appealed to the Ninth Circuit in November 2024, and appellate briefs have now been filed. In its appellate brief, the SEC seemingly retreats from an overarching "shadow trading" theory, instead hanging its hat on a breach of contract theory based on language in Panuwat's agreement prohibiting the use of any of Medivation's material nonpublic information to trade in the securities of another publicly traded company. This pivot

aligns with the new administration's focus on bread-and-butter fraud and suggests that non-contractual shadow trading theories may take a back seat for now.

f. PCAOB

The PCAOB enters 2026 amid significant changes that will impact inspections and enforcement in the year ahead. The SEC approved a 2026 PCAOB budget of $362 million, a 9.4% decrease year over year, with notable reductions to Board member compensation, while the SEC reassesses the Board's strategic plan and operations. Substantively, the effective date of QC 1000—the PCAOB's "landmark" quality control standard modernizing firm-wide systems, including annual evaluations and an external quality control function for the largest firms—was deferred one year to December 15, 2026 after stakeholder feedback on implementation burdens. Meanwhile, legal headwinds remain significant: the Supreme Court's decision in *SEC v. Jarkesy, see infra*, constrains in-house penalty adjudications. Ongoing "John Doe" challenges to the PCAOB's disciplinary process through in-house adjudication based on the Supreme Court's *SEC v. Jarkesy* decision and other constitutional arguments, potentially threaten PCAOB's adjudicatory pathway, given the PCAOB's lack of statutory authority to litigate in federal court. These dynamics follow a turbulent 2025 in which PCAOB Chair Erica Williams resigned, and after soliciting candidates for all PCAOB Board seats, the SEC appointed Demetrios Logothetis as Chairman and three officials in the Trump Administrationto the remaining Board seats on January 30, 2026.

Against this backdrop of a reduced budget and increased SEC scrutiny, audit firms should expect a measured shift in PCAOB enforcement with the focus remaining on critical audit failures. The amended contributory liability standard (Rule 3502)—lowering the scienter threshold from recklessness to negligence—may provide fodder for increased enforcement activity, although as we have stated previously, the PCAOB may lack a statutory basis to amend this threshold. Market participants should also plan for inspection focus influenced by QC 1000's frameworks, including risk-based design and governance enhancements, despite the delayed effective date, as the Board and staff integrate the standard's concepts into interim supervision, remediation expectations, and root-cause analyses. Finally, the SEC's 2026 budget order underscores a heightened SEC check on PCAOB stewardship of the accounting support fee, which could affect the pace and scope of PCAOB programs over the coming year.

g. Update on Jarkesy

After the Supreme Court held in *SEC v. Jarkesy*, 603 U.S. 109 (2024) that the SEC could not pursue civil monetary penalties through an administrative action – part of a larger trend of decisions curtailing administrative authority – the future of the SEC's in-house enforcement appeared uncertain.

A recent district court decision, however, declined to extend *Jarkesy's* holding to the SEC's use of administrative courts to pursue securities industry bans. Nonetheless, continued attempts to expand *Jarkesy* are expected, and the decision has already been applied to a number of other agencies, including the Department of Labor, the FCC, and the FAA.

h. Potential Semi-Annual Reporting Changes

The SEC has announced its plan to propose rules that would reduce financial reporting requirements from quarterly to semi-annually.

As Commissioner Uyeda recently noted, the plan, if adopted, would bring the U.S. into alignment with foreign jurisdictions, including the United Kingdom and European Union, which both have semi-annual reporting requirements. Proponents of semi-annual reporting argue this will reduce regulatory oversight and expenses associated with quarterly reporting and allow investors to focus on longer term performance. Detractors suggest this may reduce transparency.

***

This past year saw a turbulent reshaping of financial regulatory policies and securities enforcement. That said, in the coming year we expect the SEC to continue on the path forged in 2025. The Agency and peer regulators are potentially signaling new guidance pertaining to cryptocurrency and block-chain trading, and will likely maintain enforcement of traditional fraud while avoiding novel prosecution strategies to encourage innovation. We will continue to provide updates on important developments as the year progresses.

CONGRESSIONAL INVESTIGATIONS: YEAR IN PREVIEW AND WHAT TO EXPECT IN 2026

BY MATTHEW E. MILLER , DANIEL LEVIN , SHAYONNA CATO, CAROLINE HOLLIDAY AND DEBORAH WILLIAMS

As Congress enters the mid-term election year, organizations across sectors should prepare for intensified congressional investigations. (For a discussion of some of the key differences between congressional and executive investigations see last year's post here.) With artificial intelligence reshaping entire industries, DEI programs under sustained political and legal vigilance, and the Trump administration reshaping federal enforcement priorities, congressional committees are poised to wield their investigatory powers with unprecedented vigor. The targets are broad, including: technology firms navigating an uncertain AI regulatory landscape, higher education institutions facing funding threats tied to diversity policies, climate-focused nonprofits scrutinized for alleged foreign influence, and health insurers under the microscope for rising costs and opaque algorithmic decision-making.

SPECIAL CONSIDERATIONS IN AN ELECTION YEAR

Over the last 20 plus years, congressional investigations have been increasingly political, regardless of the party in control of each house. That said, the political nature of investigations only increases during election years, and we expect that to continue this year. Moreover, while the effects of the mid-terms on committee leadership will not be directly felt until next year it is likely that the current minority leadership may be signaling its own round of politically inspired investigations for next year if they are poised to take over the majority (we expect, for example, letters demanding preservation of documents relating to various matters). With that proviso, below are the main initiatives we anticipate from Congress:

Technology

Technology, and especially artificial intelligence ("AI"), was a major focus for the first session of the 119th Congress. This year, Congress will likely continue exploring the impact of AI on our lives and begin probing more deeply the contours of a regulatory scheme for AI. Congressional Republicans will also likely continue their efforts to increase data privacy protections, fortifying American systems against national security threats. Other key areas to watch include the impact of technology and social media on children and digital asset regulation.

Artificial Intelligence

With the recent explosion of artificial intelligence use across society, Congressional committees held several hearings in 2025 about AI use in the American economy. In September 2025, the

Subcommittee on Cybersecurity, Information Technology, and Government Innovation of the House Oversight and Government Reform Committee held a hearing titled "Shaping Tomorrow: The Future of Artificial Intelligence," highlighting how AI is increasingly being used in multiple sectors, including healthcare and agriculture. It is also clear that Congress remains concerned about maintaining American dominance in this area, against adversaries like China and Russia, especially as it relates to advanced AI chips. This year, we can expect that Congress will continue diving into these areas.

Social Media

Last year, we noted that Senator Ted Cruz, as head of the Senate Committee on Commerce, Science, and Transportation could wield substantial influence related to AI-related investigations. As recently as January 15, 2026, Senator Cruz led a hearing focused on the intersection between technology, social media, and children's health, representing Congress's continued efforts to investigate the dangers of the internet and technology on children.Over the course of the rest of the year, we can expect legislators ongoing congressional investigations, perhaps related to possible legislation attempting to lessen these dangers (e.g., Senator Cruz's and Senator Brian Schatz's reintroduction of the Kids Off Social Media Act (KOSMA), legislation that aims to protect children from the harmful effects of social media by restricting children's access and the functionality of social media applications themselves).

Diversity, Equity, and Inclusion ("DEI") Practices

To kick off the dismantling of federal DEI infrastructure, the second Trump Administration issued a number of Executive Orders ("EO"'s) directing agencies to terminate DEI offices, programs, contractors, and related curricula—realigning compliance expectations across grant-making and oversight functions that touch higher education (to be discussed further below). Guidance from the Office of Management and Budget ("OMB") and the Office of Personnel Management ("OPM") directing agencies to pause activities implicated by the EO's and to operationalize closures of DEI units signaled that federal program administration and grant oversight would be filtered through a new anti-DEI lens. We should expect congressional inquiries into DEI-linked policies in aid, hiring, programming and ceremonies to likely broaden.

Congress's 2025 approach to DEI followed the December 2024 House staff report condemning universities' responses to antisemitism and urging aggressive Title VI and Clery Act enforcement, funding consequences, and increased "viewpoint diversity." As a continuation of the "diversity" discussion, on June 26, 2025, the Subcommittee on Health Care and Financial Services of the Committee on Oversight and Government Reform of the U.S. House of Representatives (the "Subcommittee") hosted a hearing titled, "Sacrificing Excellence for Ideology: The Real Cost of DEI". Majority members argued that DEI initiatives were divisive, produced fraud in federal programs, undermined meritocracy in sectors such as healthcare and education, and violated civil rights laws. While Minority members defended DEI initiatives as necessary when addressing systemic inequities within, e.g., the healthcare and education sectors, Majority members doubled down on the argument that legal action against companies and universities that implement DEI initiatives should be taken.

Congress has complemented the executive-enforcement posture by probing into "illegal activity" within advocacy groups: fraud on the basis of DEI-"friendly" policies or engagement. On April 2,

2025, the House Judiciary Committee, the Committee on House Administration, and the House Committee on Oversight and Government Reform released a joint interim staff report targeting ActBlue, a major Democratic fundraising platform.

These congressional hearings and subsequent reports condemning the use or even consideration of DEI are in line with what to expect in 2026. More "illegal DEI" inquiries will target advocacy groups, affinity programs, hiring, and educational scholarships and fellowships. Congressional committees will press these institutions for lists of DEI-linked programs and donor restrictions—leveraging EO-termination mandates to frame noncompliance as grounds for restricting federal funds.

Higher Education

Throughout 2025, Congressional committees amplified scrutiny of universities' handling of antisemitism, gender policies, and DEI spending, previewing expansive document demands across disciplinary records, curricula, and donor-funded initiatives. Congress doubled down on DEI-overhauls via a slate of higher education bill proposals and legislation, contemporaneously with investigations into institutions with programs and research that prioritize DEI, critical race theory ("CRT"), gender-sex disciplines, and more. We should expect Congress to use these investigations into higher education to build the factual and political predicate for further executive and legislative enforcement, and to pressure institutions with the immediate threat of funding consequences along the way.

In June 2025, the House Judiciary Committee requested Brown University's President to hand over all internal memos related to a disciplined student who used AI to determine what Brown employees did and the reasoning behind Brown's tuition. This student categorized Brown's staff in three categories, one being "DEI jobs." The Committee stated their concerns were due to "whether Brown University and other Ivy League institutions are engaging in anticompetitive pricing practices," finding reason for more oversight to combat these "serious concerns."

On November 6, 2025, the House Judiciary Committee released an interim staff report, alleging that George Mason University (GMU) likely violated the Civil Rights Act by "using racial quotas and racial demographic balancing in faculty hiring to advance GMU President Dr. Washington's diversity, equity, and inclusion (DEI) initiative." A further probe into GMU campuses allowed the Committee to gather more evidence supporting their allegations, creating more room for oversight to pressure colleges and universities to align hiring and funding structures with federal mandates. This groundwork foreshadows an escalated congressional effort into targeting and cracking down on DEI-based infrastructure in 2026.

This year, expect the House Education committees—working in tandem with Judiciary, Oversight, and Science committees—to use investigative pressure to assist the Trump administration in achieving its purported goal of "enforce[ing] civil rights laws to end illegal preferences and discrimination espoused by DEI programs." Title VI investigations will continue to tee up threatened funding freezes and negotiated resolution agreements, drawing on agency probes and committee hearings that highlight alleged failures to ensure nondiscriminatory access to programs, scholarships and fellowships. These investigations are designed to create an evidentiary record and political momentum to support legislation that conditions or restricts funding, while also chilling

campus policies through reputational pressure and grant-risk narratives. Indeed, the consequences of these investigations are already in play: threatened blockades on new grants, potential loss of tax-exempt status, and litigation exposure even where institutions initially comply.

Climate-Focused Nonprofits

In 2025, Congress continued its efforts to investigate nonprofits associated with combatting climate change, and we do not expect those efforts to diminish in 2026. Republicans will likely continue such investigations, focusing on allegations of misuse of taxpayer funds and improper foreign influence.

A major focus of the House Oversight and Government Reform Committee ("House Oversight Committee") has been the eight nonprofits that received grants from the Greenhouse Gas Reduction Fund, established under the 2022 Inflation Reduction Act, former President Biden's landmark climate law. In March 2025, the House Oversight Committee intensified its investigation into the so-called "Green New Deal scam" and demanded documents and communications from the recipient nonprofits related to the funding they received. The EPA also froze the funds around the same time, sparking lawsuits and a counter-investigation by Democrats into the freeze.

More recently, the House Judiciary Committee opened an investigation into whether the Environmental Law Institute (ELI), a nonprofit research and education center working to improve environmental law and policy, is improperly influencing federal judges presiding over climate change-related lawsuits via its Climate Judiciary Project (CJP). Per the ELI's website, the CJP aims to provide judges with authoritative, objective, and trusted education on climate science. Members of the Committee have thus far sent letters to judicial groups and lawyers seeking information relating to communications with the ELI.

Looking farther afield, several representatives have called for investigations related to allegations that China's funding of certain U.S.-based climate nonprofits is designed to manipulate American policy in favor of Chinese "green" technology. Via a November 2025 letter to the Department of Justice (DOJ), representatives sought probes into potential violations of the Foreign Agents Registration Act (FARA) and abuse of tax-exempt status by the climate nonprofits.

Healthcare

Given all of the debate surrounding the ACA Premium Tax Credits and the government shutdown that followed in 2025, healthcare and healthcare costs are likely to be an area of renewed focus for Congress in 2026. As a result, hospitals, insurers, and pharmaceutical companies are likely to face increased scrutiny, especially as "affordability" continues to be a sticking point for the American public and the Trump administration.

For example, on January 22, 2026, Congress convened top executives from major insurers such as UnitedHealth Group, CVS Health, Elevance Health, The Cigna Group, and Ascendiun, to discuss health insurance affordability. During the hearing before the Subcommittee on Health of the Committee on Energy and Commerce, Representatives from both parties pressed the executives on issues related to the rising cost of drugs, insurance premiums, preventative care versus diagnostic care, and the lack of competition in the insurance industry. As the year progresses, Congress's investigation into this area will likely expand.

As noted above, technology and AI concerns are also likely to be a focus within the healthcare space. During the January 22, 2026 hearing, Representative Robin Kelly questioned Stephen Hemsley, UnitedHealth Group's CEO, about reports citing an increase in "inappropriate" and unregulated AI authorization tools by UnitedHealth Group, which often result in authorization denials. As AI usage increases, in healthcare as well as other sectors, Congress will have to be prepared to swiftly investigate and respond to the resulting risks and potential harm presented by use of the rapidly developing technology.

In 2026, we can also expect Congress to continue investigating the care and treatment of transgender youth. While there has been little public investigative activity in this area as of late, we would not be surprised if Congress's efforts intensify as the year progresses, especially as investigations led by the Department of Justice and the Department of Health and Human Services develop.

* * *

Companies, investors, scientific and educational institutions and non-profit organizations should expect the current Congress to aggressively use its investigatory powers to help forward the Republican agenda and the priorities of the Trump Administration in the areas we discuss above. We will continue to follow the activities of various congressional activities as the year progresses.

FALSE CLAIMS ACT TRENDS AND EXPECTATIONS FOR 2026

BY YONI BARD, CAROLINE DONOVAN, ANTHONY D. MIRENDA, DAVID G. LAZARUS, NATALIE PANARIELLO, SHAYONNA CATO, AND LANGIE CADESCA

The False Claims Act ("FCA") has long served as the federal government's workhorse for fraud investigations and enforcement. Perhaps more than any time in recent years, the executive branch writ large continues to signal that (1) it understands the potential breadth of the FCA as an investigations and enforcement tool for the government and whistleblowers, and (2) it plans to wield all available tools – including the FCA – to accomplish its stated priorities. Given the significant airtime expended nationally on the current administration's likely use of the FCA, whistleblowers and their attorneys have also signaled a strong desire to identify and pursue state and federal FCA litigation.

We anticipate a continued steady flow of health care and life sciences FCA investigations, as well as robust use of the FCA and its related investigatory tools (e.g., compulsory process) in: the trade, tariff, and customs space; in connection with investigations surrounding diversity, equity, and inclusion practices alleged to be discriminatory by the government or purported whistleblowers; and government contracting and cybersecurity. We also expect that State Attorneys General will continue and increase their use of state analogs to the federal FCA.

I. THE ADMINISTRATION'S EMPHASIS ON THE FALSE CLAIMS ACT IN FRAUD ENFORCEMENT

From the outset, this administration has been vocal about its commitment to combatting fraud in government programs. Last year, the DOJ Criminal Division declared that "[r]ampant healthcare fraud and program and procurement fraud drain our country's limited resources." More recently, when announcing another record breaking year of FCA enforcement actions, Deputy Attorney General Todd Blanche stated that "[s]topping rampant fraud is a top priority, and . . . the False Claims Act remains one of the government's most powerful weapons against fraud."

Executive activity in 2025 aligned with that announced priority. In July 2025, the DOJ and the Department of Health and Human Services ("HHS") announced the renewal of the DOJ-HHS False Claims Act Working Group, which was initially formed in December 2020. The announcement identified six priority enforcement areas for the Working Group: (1) Medicare Advantage; (2) pricing of drugs, devices, and biologics; (3) barriers to patient care; (4) kickbacks tied to products paid for by federal health care programs, including drugs, medical devices,

and durable medical equipment; (5) materially defective medical devices; and (6) manipulation of electronic systems containing health records.

In August 2025, the DOJ and the Department of Homeland Security ("DHS") launched another cross-agency group, the Trade Fraud Task Force, to pursue enforcement actions targeting tariff evasion. As described below, fraud related to trade, tariffs, and customs is an area of increased interest for the Trump administration, with some significant FCA recoveries announced over the last several months.

Further, as we detailed previously, the DOJ released updated guidance for its Corporate Whistleblower Awards Pilot Program, expanding the number of "subject areas" in which tips could lead to forfeiture. The expansion of this program creates a new reporting avenue for whistleblowers, on top of the frequently used qui tam provisions in the FCA and is yet another indicator that the government is encouraging potential whistleblowers to uncover fraud and rewarding those who do.

As we recently reported, on February 26, 2026, the Centers for Medicare and Medicaid Services ("CMS") announced a package of major anti-fraud actions, including a $259.5 million deferral of federal Medicaid funding to Minnesota, a nationwide six-month moratorium on new Durable Medical Equipment, Prosthetics, Equipment, and Supplies ("DMEPOS") supplier enrollment in Medicare, and a Request for Information soliciting stakeholder feedback on potential regulatory and programmatic changes that could be included in a future proposed rule titled "Comprehensive Regulations to Uncover Suspicious Healthcare," or the "CRUSH Rule." Together, these actions signal the administration's intent to significantly expand CMS's fraud prevention, detection, and enforcement capabilities across all major federal health care programs.

II. PRIORITY AREAS OF FCA ENFORCEMENT

a. Trade, Tariff, and Customs Fraud

In the DOJ's May 2025 memorandum titled "Focus, Fairness, and Efficiency in the Fight Against White-Collar Crime," the DOJ stated that it would prioritize enforcement of international trade, tariff, and customs fraud, which can give rise to liability under the reverse false claims provision of the False Claims Act that applies when an entity underreports or underpays amounts owed to the government.

On July 10, 2025, the DOJ combined resources from its Criminal and Civil Divisions to create a Market, Government, and Consumer Fraud Unit ("MGC Unit") within the Criminal Division's Fraud Section. The MGC Unit's stated goal is to "investigate[] and prosecute[] offenses involving fraud and manipulation that harm U.S. markets and investors, schemes to defraud government benefit programs, evade tariffs, and/or to procure government contracts through fraudulent means, and complex consumer and investment frauds targeted at Americans." Soon after, on August 29, 2025, the DOJ and DHS launched a cross-agency Trade Fraud Task Force to bring together prosecutors from the Civil and Criminal Divisions with investigators from U.S. Customs and Border Protection and Homeland Security Investigations. The Task Force's stated goal is to

"aggressively pursue enforcement actions against any parties who seek to evade tariffs and other duties, as well as smugglers who seek to import prohibited goods into the American economy."

Around the same time, the DOJ began announcing a series of settlements of FCA claims grounded in customs evasion, all involving Chinese imports, signaling the DOJ's willingness to rely on whistleblowers in complex trade and shipment schemes:

- On July 23, 2025, the DOJ announced a $6.8 million settlement with subsidiaries of MGI International LLC for the failure to pay customs duties on certain types of plastic resin imported from China. The settlement amount was significantly lower than the maximum penalty available because the subsidiaries voluntarily self-disclosed the violations and cooperated with the government's investigation.

- On July 24, 2025, the DOJ announced a $4.9 million settlement with Grosfillex Inc. for evading antidumping and countervailing duties on certain aluminum products from China. The case originated from a whistleblower lawsuit brought in 2020 by a former employee; the whistleblower received nearly $1 million of the settlement.

- On December 18, 2025, the DOJ announced a $54.4 million settlement with Ceratizit USA LLC for failing to pay customs duties on tungsten carbide products from China, which has been touted as the largest FCA settlement involving customs fraud allegations. This FCA case was initially brought in 2022 by a whistleblower who received a payout of nearly $10 million.

All of these resolutions involved tariffs that have been in place for years and began with investigations or disclosures that predated this administration. Regardless, given the centrality of tariffs to President Trump's foreign policy agenda, we expect to see increasing enforcement in this space.

The U.S. Supreme Court's decision in *Learning Resources, Inc. v. Trump*, No. 24-1287 invalidated the set of tariffs imposed by the administration pursuant to the International Emergency Economic Powers Act, but there are many tariffs imposed under other authority and the administration is acting rapidly to impose additional sweeping tariffs, so this risk area is only growing. To avoid and limit potential liability, companies should continuously monitor tariff policies, regularly perform customs risk assessments, and tighten controls around valuation, tariff classification, and country-of-origin determinations, which are the core exposure areas.

b. Diversity, Equity, and Inclusion

President Trump's January 2025 Executive Order, titled "Ending Illegal Discrimination and Restoring Merit-Based Opportunity" ("DEI EO"), instructed "all executive departments and agencies (agencies) to terminate all discriminatory and illegal preferences, mandates, policies, programs, activities, guidance, regulations, enforcement actions, consent orders, and requirements."

Fairly promptly, agencies responded to the directive in the DEI EO. On April 3, 2025, the Department of Education delivered a letter ("April 3 Letter") to state and local education agencies, requiring each to certify that it will file assurances with the Secretary of State stating it "will comply with all Federal statutes regarding nondiscrimination." The assurances require that an agency does not "violat[e] Title VI – including the use of Diversity, Equity, & Inclusion ("DEI") [] to advantage one's race over another." In May 2025, the Office on Violence Against Women ("OVW") announced a list of "out-of-scope activities," which alert applicants to certain activities OVW cannot finance. Then, in June 2025, OVM began requiring all grant funding applicants to submit a letter certifying that grant funds would not be used for those out-of-scope activities. Many other agencies, like the Department of Housing and Urban Development, Department of Transportation, and the Federal Transit Administration announced grant conditions requiring compliance with the DEI EO.

Many quickly challenged the certification requirements imposed by the DEI EO and implementing agencies, generally bringing challenges under the Administrative Procedure Act ("APA"), the First Amendment, and the Fifth Amendment. Various district courts, in turn, have preliminarily enjoined these various certification requirements. For example, in *American Federation of Teachers v. Department of Education*, the U.S. District Court for the District of Maryland vacated the certification requirement imposed by the April 3 Letter, finding that the letter violated the APA because it constituted final agency action and violated the Fifth Amendment because it was vague and failed to define "certain DEI practices." No. 1:25-cv-628 (D. Md.). These injunctions were significant victories for federally funded programs.

However, on February 6, 2026, in *National Association of Diversity Officers in Higher Education v. Trump*, which involved, in part, a facial challenge to the certification requirement within the DEI EO itself, the Fourth Circuit vacated the preliminary injunction entered by the District of Maryland.

The Fourth Circuit did so on narrow grounds, holding that the plaintiff's facial challenge was unlikely to be successful because the certification in the DEI EO "requires only that plaintiffs certify compliance with federal antidiscrimination laws, which the First Amendment doesn't confer a right to violate." The Fourth Circuit left open further as-applied challenges "if the President, his subordinates, or another grantor misinterprets federal antidiscrimination law." We would expect to see both further agency action to enforce the DEI EO against federally funded entities and contractors and lawsuits challenging the constitutionality of any such action.

The federal government will continue to rely on Title VI and the Supreme Court's decision in *Students for Fair Admissions*, to prohibit purportedly unlawful DEI programs and activities while using the False Claims Act as a basis to enforce compliance. And in its related Civil Rights Fraud Initiative, the DOJ set out to investigate and, where appropriate, pursue FCA claims against recipients of federal funds that allegedly maintain prohibited race or sex based preferences in the wake of the DEI EO. In the memorandum announcing the initiative, Deputy Attorney General Todd Blanche stated that the FCA would be the "weapon" to go after corporations and schools that "continue to adhere to racist policies."

As recently as February 19, 2026, Brenna Jenny, Deputy Assistant Attorney General, Commercial Litigation Branch, United States Department of Justice, Civil Division, reaffirmed DOJ's plan to utilize all available tools, including the FCA, to target what the administration believes are discriminatory DEI programs. DAAG Jenny also explained that it is not the underlying DEI program that is the focus of the government's investigations; rather, the government will investigate allegedly unlawful discrimination, including in hiring and promotion decisions. The government appears to be reacting to the ongoing challenges to the DEI certification requirements and has signaled its intent to press forward, even if it requires a pivot in its own terminology and messaging.

c. Health Care

Health care continues to be the primary focus of FCA enforcement by the government and whistleblowers, as discussed in our recent post on Health care Fraud Enforcement in 2026. In the fiscal year ending in 2025, settlements and judgments under the FCA exceeded $6.8 billion, and over $5.7 billion of that sum related to health care matters, including allegations of fraud involving Medicare, Medicaid, and TRICARE. In addition, on February 25, 2026, CMS announced a major crackdown on health care fraud including "deferring $259.5 million of federal Medicaid funding in Minnesota," "a nationwide moratorium on Medicare enrollment for certain . . . suppliers," and "a call to action for Americans to support fraud prevention."

In 2025, the DOJ focused on three main areas of enforcement: managed care, prescription drugs, and medically unnecessary care. In the managed care space, CMS announced that it would expand its audit of Medicare Advantage plans to address what it estimates is billions of dollars in overbilling, and the DOJ intervened in an FCA suit alleging that major insurers paid hundreds of millions in kickbacks to steer beneficiaries into specific plans. On the prescription drug front, enforcement has targeted pharmacies, telehealth platforms, and pharmacy benefit managers, with courts affirming fraud allegations where prescriptions were signed off without legitimate doctor-patient relationships. Medical necessity continues to be a cornerstone of health care fraud enforcement. The DOJ secured a $45 million settlement with a wound care provider that allegedly billed Medicare for medically unnecessary surgeries and programmed its billing software to ensure the highest-reimbursed procedures were always billed.

As we have previewed, FCA issues in the health care space were actively litigated in trial and appellate courts in 2025. This included a significant defense win on scienter in *Omni Healthcare, Inc. v. MD Spine Solutions LLC*, No. 25-1110 (1st Cir.), in which the First Circuit affirmed the district court's grant of summary judgment in favor of the defendant and found that MD Labs did not submit false Medicare claims "knowingly" under the FCA. There, MD Labs relied on test requisition forms from clinicians at Omni Healthcare as evidence that the requested PCR urine tests were reasonable and necessary. The court credited this view, finding that a laboratory may rely on such physician orders as presumptively establishing medical necessity, which presumption must then be rebutted by the relator presenting evidence sufficient "to raise a genuine dispute of material fact as to the lab's scienter."

It was an active year for health care FCA trials. This included some significant liability determinations, including against long-term pharmacies and pharmacy benefits managers. See *United States ex rel. Bassan v. Omnicare, Inc.*, No. 1:15-cv-04179 (S.D.N.Y.) (on appeal); *United States ex rel. Behnke v. CVS Caremark Corp.*, No. 14-cv-824 (E.D. Pa.) (on appeal). There were also some defense wins, including in the government-intervened matter *United States ex rel. Devarapally v. Ferncreek Cardiology, P.A.*, No. 5:17-cv-616-FL (E.D.N.C.), relating to alleged medically unnecessary cardiac procedures.

On damages, we saw some signals of restraint on outsized awards. In *United States ex rel. Taylor v. Healthcare Associates of Texas*, LLC, No. 3:19-cv-02486-N (N.D. Tex.), defendants successfully challenged a $450 million award as constitutionally excessive, holding that applying the FCA's per claim civil penalties would violate the Excessive Fines Clause of the Eighth Amendment given the gravity of the conduct and the disparity between minimum statutory penalties (nearly $300 million) and actual damages. The court instead opted to impose a reduced civil penalty equal to treble damages, resulting in a total judgment of around $16.5 million, plus post judgment interest.

And in what will be a key case to watch in 2026, *United States ex rel. Penelow v. Janssen Products LP*, an appeal is currently underway in the Third Circuit, as the defendant challenges a $1.6 billion verdict relating to allegedly false and misleading claims about the safety and efficacy of certain prescription drugs. Notably, the DOJ has filed a brief in that appeal arguing, in part, that off-label promotion does not alone establish FCA liability.

FCA claims in the health care industry show no signs of decline. As we previously observed, heightened focus on areas such as wound care reimbursement and Medicare Advantage will help health care remain the busiest area for FCA enforcement. DAAG Jenny recently outlined several areas of enforcement attention, including defective medical devices, skin substitutes, and network adequacy for managed care plans. DAAG Jenny also addressed FCA enforcement as the keynote speaker at the Federal Bar Association's Qui Tam conference, where she emphasized that health care has been a very active area for FCA enforcement, particularly regarding managed care, drug pricing, and unnecessary services. She also confirmed DOJ's continued reliance on data analysis to identify FCA enforcement targets, noting that if a company receives a Civil Investigative Demand, it is safe to assume that data analysis has occurred.

d. Private Equity and State AGs

States continue to maintain active state false claims enforcement dockets across a range of industries, with recent statutory amendments strengthening enforcement tools at the state level. For example, 2025 amendments to the Massachusetts False Claims Act under House Bill 5159 impose new disclosure obligations on private equity firms, real estate investment trusts, and management services organizations connected to health care portfolio companies. Under the expanded state law, entities

with an "ownership or investment interest" – a term defined broadly to include direct or indirect equity stakes exceeding 10%, interests held by investor pools, or interests held by private limited partnerships employing investment strategies to earn returns – may now face liability for False Claims Act violations committed by their affiliated health care providers. The statute requires disclosure of any known violation within 60 days yet leaves undefined when an investor "knows about" or has "identified" such a violation. This creates substantial uncertainty for companies attempting to navigate internal investigations and meet compliance timelines, requiring accelerated engagement of counsel.

e. Government Contracting and Cybersecurity

The DOJ has intensified its use of the FCA to pursue government contractors and vendors for alleged cybersecurity misrepresentations and failures. The DOJ uses the FCA to enforce federal cybersecurity requirements across a wide array of matters, including cases involving failing to comply with required cybersecurity standards, misrepresenting cybersecurity controls and practices, failing to monitor cybersecurity systems, and failing to report cyber incidents and breaches in a timely manner.

In 2025, the DOJ announced a new record: nine cybersecurity-related FCA settlements (including one from late 2024), surpassing the total number of such settlements reached during the entire Biden administration. These settlements also illustrate the wide array of government contractors at risk of cybersecurity FCA enforcement, with defense contractors, universities and research institutions, health care services contractors, IT services companies, life sciences companies, and private equity firms among the settling parties. According to recent remarks by DAAG Jenny, whistleblowers have played a central role in cybersecurity FCA enforcement.

Five of the nine settlements were initiated by internal whistleblowers. Four of those settlements related to the failure to comply with cybersecurity agreements with the Department of Defense ("DoD"), and the other concerned genomic sequencing systems sold to the government, which contained cybersecurity vulnerabilities.

Given the DOJ's enforcement posture, organizations doing business with the federal government should prioritize rigorous cybersecurity compliance, accurate self-assessments, and working with legal counsel to provide prompt reporting of cyber incidents to mitigate FCA exposure.

III. DEVELOPMENTS IN THE COURTS

Zafirov and the Continued Challenge to the FCA's Constitutionality

At the tail end of 2025, the Eleventh Circuit heard oral argument in *United States ex rel. Zafirov v. Florida Medical Associates LLC*, No. 24-13581 (11th Cir.). The case is on appeal from the September 2024 district court ruling that the FCA's qui tam provisions are unconstitutional under Article II's Appointments Clause (previously covered here).

During oral argument, the panel seemed to view a qui tam relator's authority as "significant," noting that filing a suit on behalf of the United States and triggering a duty to investigate carries real weight. At the same time, the panel appeared less certain on whether a qui tam relator occupies a "continuing position," acknowledging that once the government declines intervention the case proceeds like any other private civil suit. This suggests that the outcome may hinge on how the panel resolves that second element.

It is also possible that the court's decision will narrow or sidestep aspects of the district court's ruling. The panel expressed interest, for instance, in broader Article II theories, such as the Vesting Clause or the Take Care Clause. The court also probed the DOJ on whether it had refined its position since the opening brief – now emphasizing the absence of a "continuing position" while softening its earlier submission that private citizens can never be "officers" for Article II purposes.

Until a decision is reached by the Eleventh Circuit, the U.S. District Court for the Middle District of Florida is alone in its holding. Every circuit court to consider the Appointments Clause issue has upheld the FCA's qui tam provisions, although the constitutional question is now on appeal before the Third and Sixth Circuits. Meanwhile, other district courts within the Eleventh Circuit have declined to follow *Zafirov* absent a circuit decision.

Government Interventions to Dismiss under 31 U.S.C. § 3730(c)(2)(A) Post-Polansky

In 2023, in the case *United States ex rel. Polansky v. Executive Health Resources, Inc.,* the Supreme Court held that the government may intervene in a previously declined FCA case in order to dismiss it over a relator's objection.

Since then, the topic has been top-of-mind for FCA defendants in non-intervened cases. More recently, we have started to see some indicators that post-declination intervention in order to dismiss may be picking up steam. This includes recent comments from DAAG Jenny that DOJ will exercise its authority under 31 U.S.C. § 3730(c)(2)(A) in "appropriate cases." Identifying what constitutes an "appropriate case" is fact-specific, but the government has indicated that it would include cases where the government determines the relator's case lacks merit as well as cases involving previously disclosed or investigated conduct (perhaps a species of cases not dismissed under the existing public disclosure bar). DAAG Jenny stated that the government was responsible for 25 FCA dismissals under § 3730(c)(2)(A) in 2025 and noted that number does not reflect the full extent of the government's influence – namely, instances where a relator decides not to pursue a case after discussing it with the government.

Post-*Polansky*, we have seen only a few reported decisions concerning (c)(2)(A) dismissals, though those decisions are informative as to the factors militating in favor of dismissal. In *United States ex rel. Vanderlan v. Jackson HMA, LLC*, the U.S. District Court for the Southern District of Mississippi granted the government's motion to dismiss FCA counts under § 3730(c)(2)(A). Giving "substantial deference" to the government's arguments, the court emphasized that the claims

"were never [the relator's]" and that the Executive retains broad discretion to end a suit that would not vindicate the government's interests, particularly where the relator presses a novel theory—here, that alleged "patient dumping" in violation of the Emergency Medical Treatment and Labor Act could support FCA liability via false certifications. The court also rejected the relator's demands for discovery or an evidentiary hearing as prerequisites to dismissal, reading § 3730(c)(2)(A) and *Polansky* to require notice, an opportunity to be heard, and a reasonable government explanation before granting dismissal – not a mini-trial.

In *United States ex rel. Vermont National Telephone Co. v. Northstar Wireless LLC*, a magistrate judge recommended dismissal under § 3730(c)(2)(A), stressing that the suit should vindicate the government's interests even if the relator presented a contrary assessment. The litigation stemmed from an FCC spectrum auction, in which certain bidding credits were available to small businesses. The relator alleged that competitors at the auction misrepresented their small-business eligibility in order to obtain bidding credits. The magistrate judge gave substantial deference to the government's "reasonable argument for why the burdens of continued litigation outweigh its benefits." Specifically, the government pointed to insufficient evidence of fraud, significant doubt about proving damages given that no credits were ever awarded, and significant resource burdens from discovery and privilege issues. Quoting *Polansky*, the magistrate judge explained that dismissal should be granted "in all but the most exceptional cases," which this was not. The district court has not yet adopted the recommendation of the magistrate judge.

That, in each case, the government's views on dismissal were afforded substantial deference is not surprising. We will continue to monitor the incidence of (c)(2)(A) dismissals as litigants – and the government's – comfort increases post-*Polansky*.

Scope of Government Funding under Wisconsin Bell

Entities participating in programs where even a slice of funding comes from the Treasury may find themselves within the FCA's reach. In *Wisconsin Bell, Inc. v. United States ex rel. Heath*, No. 23-1127, the Supreme Court held that E Rate reimbursement requests can qualify as FCA "claims" because, in the relevant years, the United States transferred more than $100 million from the Treasury into the Universal Service Fund, satisfying the statute's "any portion" government funding requirement. The Court emphasized that Treasury deposits – including delinquent contributions, interest, penalties, settlements, and restitution the government collected and routed through Treasury – constituted funds "provided" by the government for purposes of the FCA, even if the program otherwise relies heavily on private carrier contributions.

Concurring opinions flagged unresolved issues, including whether the FCA could reach purely private transfers compelled by federal regulation and potential Article II concerns with qui tam, leaving those questions for future cases.

Regeneron Pharmaceuticals, Inc. and But-For Causation

In *United States v. Regeneron Pharmaceuticals, Inc.*, No. 23-2086 (1st Cir.), the First Circuit addressed the 2010 amendment to the Anti-Kickback Statute ("AKS") and held that a claim "resulting from" an AKS violation is false under the FCA only if the kickback was a but-for cause of the submitted claim. The court drew on ordinary causation principles and rejected the government's argument that mere exposure to an illegal remuneration suffices, distinguishing pre amendment or separate "false certification" pathways that may not require the same causation showing. The court stressed that the amendment operates on a separate track from false certification theories and does not include a materiality element, even as it requires actual causation.

The decision deepens a circuit split with the Third Circuit's more lenient "exposure" view and aligns with the Sixth and Eighth Circuits' stricter but for causation standard – positioning the issue for potential Supreme Court review. We will continue to follow the application of the *Regeneron* standard in other FCA cases.

* * *

2025 saw significant FCA activity, including in evergreen enforcement areas like health care, and in areas of renewed priority, like tariff enforcement, and new applications in DEI. As evidenced, this administration has sounded its commitment to the FCA as a mechanism to combat fraud broadly, and we will be reviewing developments as they occur.

Law Clerk Zoe Sun contributed to this blog.

HIPAA ENFORCEMENT: A LOOK AHEAD AT 2026 INFORMED BY 2025'S INFLECTION POINTS

BY COLIN ZICK

The healthcare ecosystem has closed the book on a volatile 2025, and HIPAA enforcement has moved into 2026 with sharper edges, wider apertures, and higher stakes. Regulators spent 2025 refining the tools they use, broadening the set of entities they scrutinize, and tightening expectations around cybersecurity hygiene, vendor oversight, and the responsible use of digital technologies. At the same time, parallel enforcement—from the Department of Justice, the Federal Trade Commission, and state attorneys general—has reinforced the reality that data protection failures are not just a compliance problem; they are an enterprise risk with civil, criminal, and reputational dimensions.

WHAT 2025 SIGNALED—AND WHY IT MATTERS

In 2025, the Office for Civil Rights maintained its steady cadence on HIPAA Right of Access cases, but increasingly linked access failures to broader issues—training, audit controls, and vendor performance—resulting in corrective action plans that are deeper, more prescriptive, and longer in duration. Ransomware, extortion, and third-party compromise incidents dominated the breach landscape, and OCR acted when it observed encryption "in name only," lagging patch management, and incomplete network segmentation. These deficiencies drew scrutiny not as isolated misses, but as indicators of a security program that had failed to keep pace with anticipated threats.

Regulators also signaled less tolerance for ambiguity around tracking technologies and analytics. OCR's focus on pixel and SDK deployments continued, with an emphasis on whether regulated entities know where data flows, what identifiers are transmitted, and whether disclosures fall within HIPAA's framework or require authorization and business associate agreements. The takeaway from 2025 was that undocumented assumptions, untested vendor claims, and incomplete data mapping are no longer defensible regarding pixels.

Finally, 2025 underscored an expansion in the enforcement perimeter. The FTC's Health Breach Notification Rule enforcement and state health privacy statutes operated in the space where HIPAA does not reach—consumer-facing health apps, digital tools, and non-covered intermediaries—creating a layered enforcement environment. Covered entities and business associates increasingly found themselves accountable not only for their own controls, but for the practical downstream realities of their digital ecosystem.

THE 2026 ENFORCEMENT OUTLOOK: FIVE THEMES TO PLAN AROUND

1) Expect continued rigor on the basics.

Encryption at rest and in transit, privileged access management, multifactor authentication, vulnerability remediation timelines, and incident response playbooks remain fundamentals. For documentation, you need logs that prove controls are enabled and effective, metrics showing patching intervals and exception management, and board-level reporting that demonstrates oversight of security performance, not just policy adoption.

2) Vendor risk management will be judged, and the metric will be outcomes.

OCR and parallel enforcers will look past contract clauses to confirm that providers know which vendors touch protected health information, that security representations have been validated, and that terminations, substitutions, and subcontractor changes are traceable. A living, risk-based inventory, periodic testing of vendor controls, and clear escalation paths for vendor incidents will be essential.

3) Digital health and tracking technologies will remain enforcement priorities.

Can you prove your pixels do not disclose PHI without authorization? Anticipate diligence records on data elements captured, IP address treatment, unique identifiers, and any fingerprinting, with corresponding legal rationales and BAAs where appropriate. Where consent is implicated, regulators will assess whether the consent is specific, informed, and technically enforced.

4) The line between HIPAA enforcement and white-collar risk will continue to blur.

Expect increased coordination between OCR, DOJ, and state authorities when breach investigations uncover wire fraud, identity theft, kickbacks facilitated by data misuse, or false statements to regulators and patients. When cyber incidents intersect with claims data, utilization records, or patient enrollment information, healthcare organizations should assume that criminal exposure for individuals—not only corporate liability—will be assessed.

5) Artificial intelligence will move into everything.

As health systems implement AI for scheduling, documentation, triage, and revenue cycle, regulators will probe training data provenance, access to PHI within model workflows, and the adequacy of role-based controls and human oversight. Documentation of purpose limitations, output monitoring, and error handling will be necessary to demonstrate compliance with HIPAA's minimum necessary standard and safeguards.

RULEMAKING AND GUIDANCE: WHAT TO WATCH

On the policy front, organizations should watch for continued alignment of health privacy frameworks where HIPAA intersects with other federal and state regimes. Expect additional clarity around reproductive health-related disclosures, the ongoing harmonization of 42 C.F.R. Part 2 confidentiality rules with HIPAA's structure, and further articulation of cybersecurity expectations through HHS performance goals and sector-specific guidance.

PARALLEL ENFORCEMENT: FTC, STATE AGS, AND LITIGATION PRESSURES

The FTC will continue to treat undisclosed data flows and misleading privacy claims as deceptive practices, particularly in the non-covered app and device ecosystem, while state attorneys general leverage state health privacy and general UDAP laws.

At the same time, class actions will track regulatory theories, with plaintiffs emphasizing allegedly inadequate security controls, misrepresentations in privacy notices, and harms tied to identity abuse and out-of-pocket mitigation costs.

The practical result is concurrent exposure: a single incident can trigger OCR inquiry, consumer litigation, FTC examination, and state AG scrutiny.

PRACTICAL STEPS FOR 2026 READINESS

The organizations best positioned for 2026 will treat HIPAA not as a statutory minimum, but as a floor within a broader risk framework. This starts with disciplined governance: board-level dashboards that quantify security performance, regular briefings that tie threat intelligence to control health, and clear accountability for vendor oversight, data mapping, and product review.

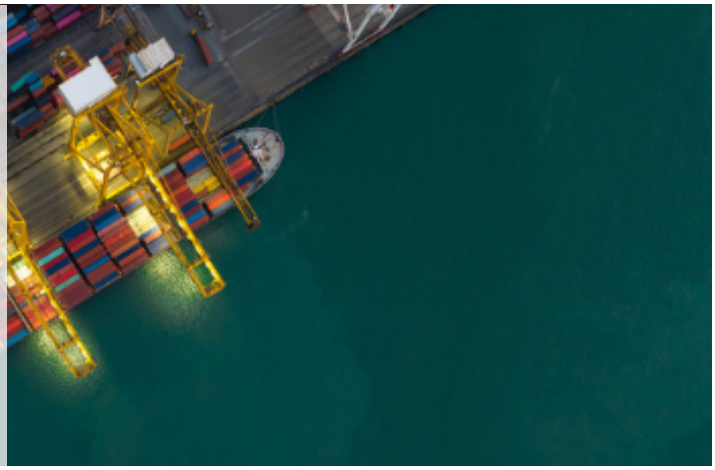
This effort continues with operational excellence: tested incident response across ransomware and extortion scenarios, tabletop exercises that include legal, communications, clinical operations, and revenue cycle, and documented learning loops that convert findings into budgeted remediation.

Organizations also need principled product design: formal reviews for any new data-collecting technology—pixels, SDKs, AI tools, connected devices—before deployment, with monitoring to confirm that configurations remain compliant as vendors update code.

Finally, entities should prepare for investigations as though they are inevitable: preserve logs and artifacts, maintain chronologies and decision records contemporaneously, and ensure counsel can demonstrate why the chosen safeguards are reasonable and appropriate for the organization's risk profile.

* * *

2025 IN REVIEW: KEY DEVELOPMENTS WITHIN INTERNATIONAL TRADE ENFORCEMENT, AND LOOKING AHEAD TO 2026



BY ANTHONY D. MIRENDA, ADAM SAFWAT, ISA MIRZA, KATHERINE JUNG, DEBORAH WILLIAMS, AARON LOVING AND JOSHUA NACHT

The Department of Justice has undertaken a sweeping realignment of its white-collar enforcement priorities under the new Administration, with a particular focus on trade and customs fraud, and continued emphasis on existing and emerging national security threats, including those involving familiar adversaries like Iran, Russia, and China as well as those from the activities of international cartels and Transnational Criminal Organizations ("TCOs"). This post examines the key policy and enforcement developments in the area of trade and sanctions enforcement by the U.S. Department of Justice (DOJ), the Bureau of Industry and Security (BIS), and the Office of Foreign Assets Control (OFAC) in 2025 and the significance of those developments for trade and sanctions enforcement in 2026. During 2025, DOJ demonstrated its commitment to these principles by issuing several declinations in response to voluntary self-disclosures.

I. DOJ'S WHITE COLLAR ENFORCEMENT PLAN ELEVATES TRADE AND NATIONAL SECURITY RELATED CRIMES AS A PROGRAMMATIC FOCUS

On May 12, 2025, the DOJ's Criminal Division issued a comprehensive memorandum titled "Focus, Fairness, and Efficiency in the Fight Against White-Collar Crime," stating that the DOJ would "move expeditiously" to target customs fraud and safeguard the "U.S. economy, American competitiveness, and … national security." The memo outlines the Criminal Division's prosecutorial and investigative priorities to combat corporate crime, encourage self-disclosure and cooperation, and streamline investigation procedures. Following this announcement, the Justice Department pursued hundreds of fraud investigations across the tax, health care, and securities industries.

Among other areas of concern, the memo elevated trade and customs fraud as a DOJ enforcement priority. DOJ also prioritized cases involving cartel transactions, sanctions violations, and other trade violations implicating national security and American competitiveness.

The Criminal Division's policy priorities are in line with Executive Order 14157, issued in January 2025, which designated certain drug cartels as Foreign Terrorist Organizations and Specially Designated Global Terrorists, and directed the federal government to pursue the "total elimination" of cartels and TCOs. Following this guidance, the Justice Department pursued a major enforcement offensive against cartels operating within the U.S., as well as cross-bordergovernmental collaboration against prolific smuggling organizations, using a wide range of tools to pursue investigations and indictments

for money laundering schemes, fraud and smuggling violations, as well as more typical charges involving drug, weapons, and crimes of violence.

a. National Security and the DOJ's Voluntary Self-Disclosure Policy

The DOJ updated its Criminal Division's Voluntary Self-Disclosure Policy to increase transparency regarding the criteria for credit for voluntary disclosure and cooperation. The DOJ also updated the Whistleblower Awards Pilot Program to align it with its stated enforcement priorities. DOJ's stated dual aims are to encourage more reporting of violations related to trade and national security matters while also encouraging companies to engage with the Department and self-report on potential violations in these areas.

On Tuesday, March 10, 2026, the Justice Department announced its first-ever Corporate Enforcement Policy for all criminal cases, largely standardizing pre-existing corporate enforcement policies across the DOJ and updating both its enforcement priorities and the use of U.S. Sentencing Guidelines in determining prosecutorial resolution for cooperating companies.

b. Creation of the Trade Fraud Task Force

On August 29, 2025, the Department of Justice launched a cross-agency Trade Fraud Task Force (the "Task Force") to advance the America First Trade Policyissued on Inauguration Day. The Task Force's priority is to "aggressively pursue enforcement actions against any parties who seek to evade tariffs and other duties," which could include civil actions under the Tariff Act of 1930, the False Claims Act, and under Title 18's trade and conspiracy provisions. The Task Force brings together several agencies within Homeland Security, Commerce and DOJ, working with U.S. Attorney's Offices nationwide, to pursue these cases. As discussed in our prior post, the False Claims Act is proving to be a powerful tool in the administration's arsenal as it pursues fraud, including particularly trade and customs fraud. DOJ shows no sign of letting up in 2026, as Criminal Division leadership has demonstrated that they will be using all available criminal enforcement tools, including provisions of the False Claims Act explicitly targeting fraudulent activity.

II. DEPARTMENT OF COMMERCE/BUREAU OF INDUSTRY AND SECURITY (BIS): EXPORT CONTROLS ENFORCEMENT

The Bureau of Industry and Security (BIS) remains at the center of the Trump Administration's efforts to restrict the flow of sensitive technology to strategic rivals, particularly China. While the pace of new rulemakings slowed in 2025 following the departure of several longtime career officials, the Administration's commitment to aggressive export control enforcement has remained steadfast. Secretary of Commerce Howard Lutnick has pledged a "dramatic increase" in BIS enforcement activity, and recent enforcement actions indicate that BIS will increase its enforcement activity in 2026.

a. Enforcement Landscape

The past year has seen major enforcement actions underscoring BIS's aggressive posture toward violations involving proscribed Chinese entities and priority technology sectors such as semiconductor manufacturing.

The most significant enforcement action ever levied by BIS came in February 2026, when BIS announced a settlement agreement and $252 million civil penalty against California-based Applied Materials Inc. and its subsidiary, Applied Materials Korea, Ltd.—the largest penalty in BIS history. At issue was Applied Materials' export of semiconductor manufacturing equipment to Semiconductor Manufacturing International Corporation (SMIC), an Entity List designee based in China, without the required BIS licenses. The equipment—ion implanters—was assembled in South Korea using components that were either U.S.-origin or shipped from the United States. Applied Materials had argued that the machines were "substantially transformed" through assembly and testing in South Korea and therefore qualified as foreign-origin items not subject to Export Administration Regulations (EAR). BIS rejected this argument, declaring that the "substantial transformation" test used under U.S. customs laws does not apply to export control origin determinations. BIS imposed the maximum statutory penalty—calculated at twice the value of the underlying transactions—indicates that BIS gave no mitigating credit and sought to send a strong message consistent with its commitment to aggressive enforcement of China-related export controls. As part of the settlement, BIS also required two internal audits of Applied Materials' export controls compliance program, with results to be submitted to BIS, and imposed a three-year suspended denial order.

In another prominent example, in July 2025, Cadence Design Systems, Inc. reached a comprehensive resolution with both DOJ and BIS regarding the unlawful export of electronic design automation (EDA) hardware, software, and semiconductor-design technology to the National University of Defense Technology (NUDT)—a Chinese military university on the Entity List. The resolution included a guilty plea by Cadence to a charge of conspiracy to commit export control violations, approximately $117 million in criminal penalties (comprising roughly $72 million in fines and $45 million in forfeitures), and a BIS civil settlement of approximately $95 million in which Cadence admitted to 61 violations of the EAR. DOJ alleged a detailed pattern of willful violations, including the use of aliases to conceal the true end user, direct communications with NUDT personnel, and efforts to hide the destination of exports from Cadence's own compliance personnel. The criminal resolution also imposed a five-year probation period requiring annual compliance reports to DOJ and prompt reporting of any further violations. BIS's civil settlement similarly required two internal audits with results submitted to the agency.

The Cadence and Applied Materials cases illustrate several key takeaways for companies operating in high-risk sectors. Companies that fail to voluntarily self-disclose violations—especially when willful misconduct or aggravating factors are present—can expect substantial penalties. Violations involving proscribed Chinese entities, particularly those on the Entity List, and involving priority areas such as semiconductor manufacturing will be treated with the utmost severity.

b. Key Regulatory Developments

Perhaps the most consequential regulatory action was the adoption, and then suspension, of the "Affiliates Rule." Issued by BIS on September 29, 2025, and modeled on OFAC's long-standing 50 percent ownership rule, the Affiliates Rule extended export control restrictions under the Entity List and Military End-User (MEU) List to all foreign entities that are 50 percent or more owned, directly, or indirectly, by one or more listed parties. The Affiliates Rule replaced BIS's previous "legally distinct"

standard, which captured only entities specifically named on the lists or non-legally distinct affiliates such as branches, but failed to cover unlisted foreign subsidiaries. BIS emphasized that the rule was designed to close loopholes, stating that "[u]nder this Administration, BIS is closing the loopholes and ensuring that export controls work as intended." The Affiliates Rule imposes significant new compliance burdens, requiring exporters to undertake affirmative due diligence into the ownership of foreign counterparties and to treat any ownership interest by a listed party as a red flag. The rule became effective immediately, though BIS issued a Temporary General License providing limited relief for transactions involving entities in certain allied countries.

However, following meetings between President Trump and Chinese President Xi Jinping in late October 2025, Treasury Secretary Scott Bessent announced a one-year suspension of the rule's enforcement. The suspension, effective November 10, 2025, came as part of a bilateral agreement in which China agreed to suspend newly implemented rare earth export controls for one year. The rule has not been rescinded, and companies should prepare for its eventual enforcement when the suspension expires. That said, companies should follow developments closely as the rule will inevitably be the subject of further diplomatic efforts as the administration seeks to balance multiple foreign policy, national security, and trade priorities.

c. Looking Ahead

The Trump Administration has signaled that it will largely continue the Biden Administration's approach to preventing the flow of sensitive technology to China but it has indicated more willingness to balance trade and commercial considerations. The White House's"America First Trade Policy" memo calls for policies that "maintain, obtain, and enhance our Nation's technological edge" and "identify and eliminate loopholes in existing export controls." New export controls on more advanced semiconductors are expected in the near future. The Administration is also expected to expand export controls related to AI, quantum computing, biotechnology, and critical minerals, and may be more willing to impose unilateral export controls rather than seeking alignment with allied countries.

Processing times for BIS license applications have increased to their highest levels in more than 30 years, which can lead to snarled supply chains, lost sales, and difficulties onboarding foreign-national employees. Companies should therefore build in longer lead times when seeking BIS authorization.

III. DEPARTMENT OF THE TREASURY/OFAC: SANCTIONS

a. The Sanctions Enforcement Landscape

OFAC's sanctions enforcement in 2025 was marked by high-dollar penalties, individual accountability, and sustained attention on financial "gatekeepers" and process discipline. Enforcement efforts consistently resulted in multi-million dollar penalties, including one penalty of over $200 million. Russian sanctions accounted for the majority of enforcement activity through the year's end, primarily targeting facilitators of financial and real estate transactions benefitting sanctioned Russian oligarchs, though enforcement activity continued at a steady pace under the Iranian, Cuban, Crimean, Syrian,

Venezuelan, and Counter-Narcotics sanctions regimes, among others. OFAC also signaled its enforcement interest beyond the usual sectoral targets of sanctions enforcement, including through an action against a U.S.-based sports academy in February 2026.

b. Focus on Gatekeepers in the Financial Services Industry and Russia Sanctions

In its OFAC's enforcement action against GVA Capital Ltd., a San Francisco based investment firm, for violations of Russia-related sanctions, resulted in the imposition of the statutory maximum penalty of $215,988,868. OFAC found that senior level persons in the firm understood that GVA was engaging in investment management activity in the United States on behalf of a Russian Specially Designated National ("SDN"), Suleiman Kerimov. OFAC also charged 28 violations (corresponding to 28 months of non-compliance) of its Reporting, Procedures and Penalties Regulations for a failure to comply with an administrative subpoena. Coupled with substantive factors such as the direct, knowing involvement of senior management in the transactions at issue, this history of non-compliance supported OFAC's conclusion that GVA's violations were egregious, helping drive its decision to impose the statutory maximum penalty. In its enforcement release concerning the GVA penalty, OFAC announced a core aspect of its enforcement strategy going forward: a focus on financial "gatekeepers—such as investment professionals, accountants, attorneys, and providers of trust and corporate formation services, among others," who "occupy crucial financial and legal positions that place them at particular risk of knowingly or unwittingly furnishing access by illicit actors to the licit financial system."

OFAC's settlement with IPI Partners, LLC the week before, in a matter concerning transactions benefitting the same SDN, similarly saw OFAC fault IPI's incomplete disclosures to outside counsel and limited early cooperation. Likewise, OFAC was unconvinced by the "use of proxies or legal structures that may conceal a blocked person's interest" with respect to IPI's knowledge, finding that "[i]ndividuals and companies with reason to know of such circumstances cannot later claim ignorance even if a blocked person has no nominal ownership or overt role" in the transactions at issue. Ultimately finding that IPI's conduct was non-egregious but not voluntarily self-disclosed, OFAC settled for a $11,485,352 payment from the company.

OFAC's enforcement of the Russian sanctions program included enforcement actions imposing individual accountability. In November 2025, OFAC imposed a $4.6 million penalty on an individual acting through a real estate investment company King Holdings LLC to mortgage, renovate, and sell real estate owned by a person blocked under OFAC's Russia sanctions. OFAC did provide an apparent off-ramp initially, however—contacting the individual before the ultimate sale to inform them that they could apply for an OFAC license to seek authorization. When the individual continued with the project without seeking OFAC approval and further continued after receipt of an OFAC cease-and-desist letter, OFAC ultimately proceeded against the individual personally.

c. Focus on widely accessible internet platforms and the value of remediation

Widely accessible internet platforms – such as retail brokerages – present significant compliance challenges and pose potentially extraordinary sanctions exposure, OFAC's enforcement action against Interactive Brokers LLC in July 2025 illustrates how effective remediation efforts can help

mitigate penalties even in those circumstances. The Connecticut-based broker-dealer resolved 12,367 apparent violations spanning sanctions regimes for Iran, Cuba, Syria, Crimea, Russia, Venezuela, and the Chinese military-industrial complex for $11,832,136. OFAC credited the company's undertaking of an internal sanctions compliance review and ultimate voluntary disclosure to OFAC. Thus, despite a serious and extensive violations history including funds transfers to blocked Russian banks, dealings in property of blocked persons under the Venezuela and Syria Sanctions Regulations, and provision of brokerage and investment services to customers in several sanctioned countries, the company was ultimately subject only to an $11.8 million settlement payment—rather than anything close to the statutory maximum penalty of over $5.2 billion, or even the base civil monetary penalty of $60.1 million.

d. Foreign distributors, subsidiaries, and overseas staff pose sanctions compliance risks

Iran- and Cuba-related resolutions in 2025 reinforced that non-U.S. affiliates, third-party distributors, and overseas employees of U.S. subsidiaries can generate direct primary-sanctions liability. On July 8, 2025, Harman International Industries, Inc. settled for $1,454,145 after overseas employees of a U.S. subsidiary facilitated diversions to Iran of consumer audio electronics products through a UAE distributor, internally using euphemisms to mask the destination. OFAC characterized the conduct as egregious but credited voluntary self-disclosure, cooperation, and significant remediation efforts.

Similarly, on July 2, 2025, Key Holding, LLC agreed to pay $608,825 because its newly acquired Colombian subsidiary continued (post-acquisition) to coordinate 36 unlicensed shipments to Cuba, underscoring acquirer liability and the expectation that U.S. parents promptly extend sanctions compliance controls and training to newly-acquired foreign subsidiaries. These examples highlight the range of compliance risks posed by foreign distributors, foreign subsidiaries and overseas staff for U.S-based companies.

e. Broad investigative interest in sanctions compliance

While OFAC's enforcement priorities have focused on business services providers such as investment managers and financial and logistics facilitators, it has looked beyond such entities towards less obvious targets as well. In February 2026, OFAC announced a $1.7 million settlement with the IMG Academy, LLC sports training school. OFAC claimed that IMG violated its Counternarcotics sanctions regime by allegedly transacting with two individuals associated with a Mexico-based drug cartel, allowing the enrollment and attendance of the SDNs' two "student-athlete children." The lesson for private institutions that accept tuition and other financial support from international clients is that they must consider risk-based sanctions screening with respect to such potential transactions. In the settlement, OFAC noted that educational institutions must be attentive to sanctions compliance – an important word of warning especially in light of the Administration's focus on higher education in other contexts.

f. What to expect in 2026

Enforcement actions over the past year indicate three enforcement trends. Russia-related matters will continue to be in OFAC's focus, with sustained emphasis on transactions for the benefit of designated oligarchs, and special focus on market "gatekeepers." OFAC will also continue to target the conduct of

overseas affiliates, distributors, and sales staff that may enable prohibited transactions. Finally, OFAC's early-2026 actions in education and individual conduct signal a wider sphere of potential sanctions risk for private U.S. institutions that have not historically operated in high risk countries or industries. Finally, OFAC continues to firmly push for voluntary self-disclosure, early and complete cooperation, and credible remediation as avenues to potentially reduce sanctions liability. OFAC has demonstrated its willingness to impose higher penalties for incomplete responses, late or inaccurate reporting, and senior-level participation in sanctions evasion.

IV. CBP AND RELATED AGENCIES: TARIFF ENFORCEMENT

a. The Supreme Court Strikes IEEPA-Based Tariffs

Beginning in February 2025, the Trump Administration invoked the International Emergency Economic Powers Act ("IEEPA")—a 1977 statute which is one of the bases of executive authority to impose sanctions but has never before been used to impose tariffs—to levy duties on imports from Canada, Mexico, China, and eventually nearly all U.S. trading partners. Over the following months, the Administration repeatedly modified these tariffs, with rates reaching as high as 145 percent on Chinese goods and additional country-specific duties imposed on Brazil, Russia, and others.

i. The Supreme Court's Decision in Learning Resources v. Trump

On February 20, 2026, the Supreme Court issued one of its most consequential trade law decisions in decades, holding 6-3 in *Learning Resources, Inc. v. Trump* that IEEPA does not authorize the President to impose tariffs. The decision disrupted the Administration's tariff program.

The President terminated these IEEPA-based tariffs the same day, and CBP halted their collection effective February 24, 2026. The terminated tariffs encompassed virtually the entire IEEPA tariff architecture—the trafficking tariffs on Canada, Mexico, and China, the global reciprocal tariffs, the country-specific duties on Brazil and India, and the secondary tariff orders related to Cuba, Venezuela, Russia, and Iran.

The scope of the disruption, while dramatic, must be understood in context. The IEEPA-based tariffs were only one layer of a much larger tariff regime. These IEEPA tariffs were layered on top of existing tariff regimes under other statutory authorities—including Section 232 tariffs on steel, aluminum, automobiles, semiconductors, and other products, and Section 301 tariffs on imports from China and Nicaragua—none of which were affected by the Supreme Court's ruling.

As Justice Kavanaugh observed in dissent, the *Learning Resources* decision does not prevent the President from imposing "most if not all" of the same tariffs under other statutory authorities, potentially "with a few additional procedural steps." The Administration moved within hours of the decision to reimpose tariffs under alternative statutory authorities and to launch new trade investigations that would support imposition of other tariffs. The President issued a new executive order imposing a 10 percent tariff on goods from all countries under Section 122 of the Trade Act of 1974, with plans to

increase the rate to 15 percent, and launched new Section 301 trade investigations designed to maintain negotiating leverage and pressure trading partners. The legal foundation of the Section 122 tariffs is itself uncertain, as Section 122 is limited to temporary surcharges addressing "balance-of-payments deficits"—a predicate the government itself has previously acknowledged may not be satisfied by trade deficits.

ii. Refunds and Ongoing Litigation

The decision also raises immediate questions regarding the billions of dollars in IEEPA tariffs CBP collected over the past year. The Supreme Court remanded the refund process to the lower courts, and more than 1,000 suits have been filed in the Court of International Trade to preserve refund rights. Recently, in *Atmus Filtration, Inc. v. United States*, 26-cv-1259 (Mar. 4, 2026), the Court of International Trade ordered the Administration to refund IEPPA tariff duties to importers of record but suspended its ruling to give CBP an opportunity to prepare to handle the complex process of refunds. Companies that paid IEEPA tariffs should preserve all records of entries, duty payments, and tariff cost allocations, and should consult with counsel regarding administrative mechanisms to protect their refund rights.

iii. End of the De Minimis Rule

The Administration's July 30, 2025 suspension of the de minimis exemption—which previously allowed duty-free importation of up to $800 in merchandise per person, per day—remains fully in effect and represents another critical area of enforcement exposure. Following the *Learning Resources* decision, the Administration immediately signed a new executive order that re-grounds the suspension under alternative legal authorities, expressly invokes IEEPA, and directs CBP to continue collecting duties on shipments that would otherwise qualify for the statutory exemption. CBP has confirmed in subsequent guidance that all low-value shipments remain subject to full tariff obligations. The elimination of de minimis treatment has closed what was once one of the most widely used channels for duty-free importation—particularly for direct-to-consumer e-commerce shipments from China—and importers should expect CBP to actively enforce tariff collection on these previously exempt goods.

V. U.S. FOREIGN INVESTMENT RESTRICTIONS

The Committee on Foreign Investment in the United States (CFIUS) enters 2026 with enforcement firmly established as a defining feature of the regime. In 2024, CFIUS assessed a record five monetary penalties. In early 2025, the Administration issued the "America First" Investment Policy to maintain an "open investment environment" for allies and partners while protecting against threats from foreign adversaries. The policy builds on prior actions, including the Biden Administration's Executive Order 14105 and final regulations issued in October 2024 targeting outbound investment in specific technologies in "countries of concern," primarily the People's Republic of China (PRC). The designated "foreign adversaries" under the policy include the PRC (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela.

CFIUS has also demonstrated a continued willingness to pursue divestiture orders, one of the most severe enforcement outcomes available. On July 8, 2025, President Trump issued an

executive order prohibiting the acquisition of California-based Jupiter Systems by Suirui Group, a Chinese company acting through its Hong Kong subsidiary Suirui International, finding that the transaction "threatens to impair the national security of the United States." The order required Suirui to divest all of its interests in Jupiter Systems within 120 days.

In January 2026, the Trump Administration ordered HieFo Corporation, a Delaware-incorporated entity controlled by Chinese investors, to divest its acquisition of digital chips and related businesses from EMCORE Corporation—a transaction that had closed in April 2024. The President found "credible evidence" that HieFo Corporation—a Delaware company "controlled by a citizen of the People's Republic of China"—through its acquisition of Emcore Corporation's "digital chips and related wafer design, fabrication, and processing businesses," "might take action that threatens to impair the national security of the United States." The Order further concluded that no other provision of law besides CFIUS's authority under Section 721 of the Defense Production Act could "provide adequate and appropriate authority" to protect national security in this matter. While the Order does not detail the specific intelligence or strategic concerns underlying the decision, the nature of the assets involved—semiconductor chip design and wafer fabrication technology—combined with Chinese control over those assets drove the outcome. The severity of the perceived threat is further reflected in the breadth of the required divestiture, which covers all interests and rights in the Emcore Assets. Only nine such divestiture orders have occurred in the past decade, three of which have come in the past two years alone.

Looking ahead, the Trump Administration's America First Investment Policy directs heightened scrutiny of investments from "foreign adversaries," particularly China, in sectors tied to critical technology, critical infrastructure, healthcare, personal data, agriculture, energy, and real estate near sensitive sites. The Administration has also signaled an intent to move away from "overly bureaucratic" mitigation agreements, favoring outright blocking or divestiture for transactions involving foreign adversary countries. Companies and investors involved in cross-border transactions should assess their CFIUS exposure proactively, particularly where the target business touches sensitive sectors or where the investor has any nexus to a designated foreign adversary.

VI. THE IMPACTS OF FORCED LABOR PREVENTION ON U.S. TRADE POLICY

The Trump Administration has continued to make good use of the Uyghur Forced Labor Prevention Act (UFLPA) as its most potent legal tool for preventing the importation of goods made with forced labor. While the UFLPA focuses on curbing forced labor abuses against persecuted minority communities in China, the law also strengthened the ability of CBP to detain goods derived from forced labor in many other jurisdictions where forced labor poses significant challenges – in particular, Malaysia, Cambodia, Vietnam. Other countries from which imports have been flagged at high rates include Thailand, India, Bangladesh, the Philippines, and Nicaragua.

There is some debate over whether the Trump Administration is paring back UFLPA enforcement or remaining relatively consistent with efforts over previous years, and to the latter extent, whether the Administration is sufficiently building on enforcement. The law provided human rights NGOs and researchers that map forced labor risks with a more direct conduit to regulators at DHS and CBP,

and this input has been playing a sizeable role in setting the direction of CBP inspections into goods from high-risk sectors and countries. According to a 2025 report led by Laura Murphy – a leading modern slavery researcher and a former top advisor on the issue at DHS – there were periods in 2025 when detentions dropped, particularly in April and May, before returning to levels more in line with past years. In addition, the report posits that the Administration has not been proactive in adding new companies to the UFLPA Entity List. The List identifies companies that are legally presumed to be using forced labor and hence bans all of their products from entering the United States.

The vicissitudes of enforcement across time and administration aside, the rate at which detained shipments are subsequently *released* had on average hovered at about 50% before the Trump Administration, meaning shipments had a fairly significant chance of being eventually deemed free of forced labor. When the 2025 year is factored into the release rate, releases since the UFLPA went into effect drop to about 35%. But it's not yet clear whether this affirms that the evidentiary bar is being raised by Trump's CBP, or if other factors are at play.

Regardless, the release rates remain high and intimate that regulators may not yet have the resources and manpower to consistently apply the UFLPA's stringent "clear and convincing" evidentiary standard that importers are supposed to demonstrate in order to rebut a presumption of forced labor. Although there are likely situations in which importers have successfully challenged detentions that meet or fall below the statutory standard, it would be unwise for any company to conclude that enforcement is lax or unpredictable.

The UFLPA was passed with overwhelming bipartisan support in Congress and both parties see the law as a powerful mechanism for countervailing China's ambitions. Additionally, the Trump Administration's trade war with China stands to gain from consistent application of the UFLPA, insofar as many U.S. goods flow from supply chains that either originate in China or overlap with Chinese industries. The Administration is continuing to prioritize the inspection of goods in high-risk sectors that include automative manufacturing, electronics, polysilicon, apparels, and steel; and critical minerals such as lithium and copper. More commercial sectors, product types, and materials could be added in the future, and CBP continues to weigh risk mapping data provided by researchers and civil society.

The Trump Administration is also taking advantage of new bilateral and regional trade agreements to advance forced labor prevention efforts in key trading partner nations. Provisions compelling governments to take greater action against forced labor could very well figure into the reauthorization of the U.S.-Mexico-Canada Agreement, which is a key legislative priority for Congress in 2026. The USMCA, the signature trade policy of Trump's first term, included language in Articles 23.12 and 23.6 calling for closer coordination between Washington, Mexico City, and Ottawa on eradicating forced labor in North American supply chains. After the USMCA went into effect, Canada enacted a law that requires companies to report on their efforts to prevent forced labor and child labor, while Mexico's Department of Labor promulgated a regulation prohibiting the import of goods made with forced labor.

Outside of North America, the U.S.-Malaysia Agreement on Reciprocal Tradethat was signed in October 2025 also refers to forced labor obligations. Article 2.9 requires Malaysia to implement a ban on imports made with forced labor within two years of the Agreement's enforcement date. Importantly, Article 2.9 further calls for Washington and Kuala Lumpur to share best practices regarding enforcement of the UFLPA and Malaysia's import prohibitions. Similarly, with respect to the U.S.-Cambodia Agreement on Reciprocal Trade, Article 2.8 requires Phnom Penh to implement a UFLPA-like prohibition on imports. Commitments to eradicating forced labor are also referenced in the White House's new agreements with Vietnam and Thailand, and Article 1.19 of the U.S.-Bangladesh Agreement on Reciprocal Trade that was signed in February obligates Dhaka to increase the number of labor inspectors and carry out unannounced inspections to identify forced labor and child labor violations. This extends to Export Processing Zones, where regulatory regimes can be weaker and forced labor risks more acute.

With UFLPA inspections especially trained on these countries, the trade agreements are a further sign that companies will need to prioritize forced labor prevention in their policies, due diligence, risk assessment process, and the monitoring of supply chain partners.

* * *

In 2025, we saw a sweeping realignment of U.S. trade enforcement priorities and an aggressive expansion of tools used in centering those priorities. Looking ahead to 2026, we can expect the exercise of all available criminal enforcement tools, an expansion of export controls, and a widening sphere of potential sanctions risk for private institutions, all within a dynamic tariff landscape. We will continue to follow these trends as the year progresses.

For more information on Foley Hoag's 2026 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

Natalie Panariello
Associate – *Boston*
+1.617.832.1780
npanariello@foleyhoag.com

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

Jace Lee
Associate – *New York*
+1.212.812.0398
jlee@foleyhoag.com

Adam Safwat
Partner – *Washington, DC*
+1.202.261.7372
asafwat@foleyhoag.com

Joshua Nacht
Associate – *New York*
+1.212.812.0454
jnacht@foleyhoag.com

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

Marilyn Icsman
Associate – *Boston*
+1.617.832.1236
micsman@foleyhoag.com

Caroline Holliday
Associate – *Boston*
+1.617.832.3106
choliday@foleyhoag.com

Isa Mirza
Senior Adviser – *Washington, DC*
+1.202.261.7379
imirza@foleyhoag.com

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

Dalton Sousa
Associate – *Boston*
+1.617.832.1172
dsousa@foleyhoag.com

Emily Nash
Partner – *Boston*
+1.617.832.3067
enash@foleyhoag.com

Aaron Loving
Associate – *Boston*
+1.617.832.7161
aloving@foleyhoag.com

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

Adam Safwat
Partner – *Washington, DC*
+1.202.261.7372
asafwat@foleyhoag.com

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

Dan Levin
Partner – *Washington, DC*
+1.202.570.8825
dlevin@foleyhoag.com

Langie Cadesca
Associate – *New York*
+1.212.812.0418
clcadesca@foleyhoag.com

Katherine Jung
Associate – *New York*
+1.201.638.5582
kjung@foleyhoag.com

David Lazarus
Partner – *Boston*
+1.617.832.1122
dlazarus@foleyhoag.com

Isabel Celio
Associate – *Boston*
+1.617.832.1259
icelio@foleyhoag.com

Howard Weiss
Associate – *Boston*
+1.617.832.1260
hweiss@foleyhoag.com

Deborah Williams
Associate – *Boston*
+1.617.832.7170
dwilliams@foleyhoag.com

Daniel Zaleznik
Associate – *Boston*
+1.617.832.3043
dzaleznik@foleyhoag.com

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

Gilleun Kang
Associate – *Boston*
+1.617.832.7163
jgkang@foleyhoag.com

Shayonna Cato
Associate – *New York*
+1.212.812.0313
scato@foleyhoag.com

Colin Zick
Partner – *Boston*
+1.617.832.1275
czick@foleyhoag.com