

YEAR IN PREVIEW 2023

White Collar Law & Investigations



CHECK OUT THE LATEST NEWS & INSIGHTS
[White Collar Law & Investigations Blog](#)

TABLE OF CONTENTS

<u>False Claims Act Enforcement: Looking Back and What to Expect in 2023</u>	<u>3</u>
<u>2023 Trends in Criminal Tax Enforcement</u>	<u>5</u>
<u>Heath Care Enforcement: Review of 2022 and a Look Ahead to 2023.....</u>	<u>7</u>
<u>Scrutiny for the Private Sector Will Come From Both Sides of the Aisle in the 118th Congress.....</u>	<u>10</u>
<u>Previewing SEC Enforcement in 2023.....</u>	<u>13</u>
<u>Will Stakeholder Objections and Legal Uncertainty Slow and ESG Revolution?.....</u>	<u>16</u>
<u>Andrea Campbell's First Month In Office: A Review of the Review of the Attorney General's Priorities.....</u>	<u>19</u>
<u>Federal Cryptocurrency Enforcement in 2023</u>	<u>22</u>
<u>Foreign Corrupt Practices Act (FCPA) 2022 Year in Review and A Look Ahead</u>	<u>25</u>
<u>Navigating the International Trade & National Security Landscape 2023.....</u>	<u>31</u>

FALSE CLAIMS ACT ENFORCEMENT: LOOKING BACK AND WHAT TO EXPECT IN 2023

BY CAROLINE DONOVAN, NATALIE PANARIELLO, JASMINE N. BROWN

FEBRUARY 13, 2023

The False Claims Act (or “FCA”) continued to drive significant enforcement activity in 2022, especially, but not exclusively, in the healthcare sector. In 2023, we expect the government and whistleblowers to continue to prosecute and likely resolve False Claims Act matters in large numbers. In addition, we await decisions from the Supreme Court in *United States, ex rel. Polansky v. Executive Health Resources, Inc.* and consolidated cases, *United States ex rel. Schutte v. SuperValu Inc.* and *United States ex rel. Proctor v. Safeway, Inc.* Together, these cases will answer critical questions about the government’s ability to dismiss suit after declining to intervene and False Claims Act defendants’ ability to rely on objectively reasonable interpretations of regulation as evidence of intent.

2022 by the numbers

In 2022, FCA matters continued to be a fertile ground for the government and whistleblowers, though the sheer number of FCA matters did not necessarily track the dollars recovered. Thus, in 2022, the government and whistleblowers resolved 351 FCA matters through settlement or judgment—the second highest number of settlements and judgments in a single year. Despite this high volume, total FCA recoveries dipped from \$5.6 billion in FY 2021 to \$2.2 billion in FY 2022. More than \$1.9 billion of the \$2.2 billion came from resolutions of whistleblower lawsuits, resulting in \$488 million in payouts to whistleblowers.

Notably, whistleblowers filed 652 new qui tam lawsuits in 2022, a steady stream of more than 12 new cases on average each week. What this portends for 2023 awaits to be seen, but based on this data and general historical trends, the FCA will continue to be a frequently invoked enforcement tool.

Healthcare continues to be the mainstay, but not to the exclusion of other industries

Unsurprisingly, the health care industry remained the primary area of FCA enforcement in 2022, with over \$1.7 billion in settlements and judgments in matters involving drug and medical device manufacturers, durable medical equipment, home health and managed care providers, hospitals, pharmacies, hospice organizations, and physicians. Notably, several of these health care matters involved claims against individuals, consistent with the government’s stated commitment to use the FCA to pursue individuals as well as corporations.

There are pockets of other budding FCA activity. In a first under its Civil Cyber-Fraud Initiative, announced in October 2021, the government settled its first Civil Cyber-Fraud FCA matter with Comprehensive Health Service LLC (CHS) for \$930,000. The government alleged that CHS certified that it complied with the State Department and Air Force’s contract requirements and submitted claims to the State Department for the cost of a secure electronic medical record system. The electronic medical record system was intended to store the confidential identifying information of U.S. service member, diplomats, officials, and contractors working and receiving medical care in Iraq. However, the government alleged that CHS failed to disclose that it did not consistently store patients’ medical records on this secure system, and instead stores copies of the records on an internal, unsecured, network drive.

Cybersecurity is not the only non-health care area where the government’s FCA attention has increased. The government continues to pay close attention to COVID-related fraud cases, including

improper payments and lender disbursements under the Paycheck Protection Program by the U.S. Small Business Administration and improper vaccination of ineligible individuals under the Centers for Disease Control and Prevention's Pharmacy Partnership for Long-Term Care Program.

In addition to the above, we note other areas of interest for the government, including allegations of fraud in customs contracts, small business contracting, and telecommunications contracts.

Up next: A big year for the False Claims Act at the Supreme Court

The year ahead promises to be a big year for the False Claims Act, both doctrinally and practically, with the Supreme Court of the United States agreeing to hear two sets of FCA cases during its 2022-2023 term.

The first, *United States, ex rel. Polansky v. Executive Health Resources, Inc.* ("Polansky"), concerns the government's authority to dismiss a False Claims Act suit after initially declining to intervene in the action. Under the FCA, when a whistleblower files a lawsuit alleging violations of the Act, the government must decide within a specified period of time whether it wishes to intervene in the suit, in which case the government will take over prosecuting the action. If the government declines to intervene, the whistleblower may conduct the action on their own and receive up to thirty percent of any recovery. In Polansky, the government had initially declined to intervene, only to later decide, after the whistleblower's lawyers had incurred \$20 million in time and costs, to seek dismissal. The district court dismissed the action over the whistleblower's objection, and the whistleblower appealed, first to the Third Circuit, which affirmed the dismissal, and now to the Supreme Court. The Supreme Court heard argument on December 6, 2022, and will decide whether the government can seek dismissal in such circumstances and, if so, what standard courts should apply when ruling on motions to dismiss. Certainly for companies facing False Claims Act suits prosecuted by whistleblowers, the government's ability to seek dismissal of pending suits is an important protective mechanism.

The second set of cases, *United States ex rel. Schutte v. SuperValu Inc.* ("SuperValu"), and *United States ex rel. Proctor v. Safeway, Inc.* ("Safeway"), concern the FCA's scienter element. FCA liability only attaches to a defendant who acts "knowingly," which the Act defines as actual knowledge, deliberate ignorance, or reckless disregard. The defendants in *SuperValu* and *Safeway* argued that they did not "knowingly" submit false claims because they relied on objectively reasonable interpretations of relevant regulations, regardless of whether they subjectively believed that those interpretations were correct. The Seventh Circuit sided with the defendants, ruling that the defendants had not acted "knowingly" because their interpretations of the regulations were objectively reasonable, there was no authoritative guidance that cautioned against their interpretations, and their subjective beliefs were irrelevant for purposes of liability. The plaintiffs petitioned the Supreme Court to hear their appeal, and the Supreme Court granted the petitions and consolidated the appeals for argument this April.

We will follow these matters closely in the year ahead and share development as they come down.

2023 TRENDS IN CRIMINAL TAX ENFORCEMENT

BY JOANNA MCDONOUGH, EMILY NASH

FEBRUARY 14, 2023

The days of decreased IRS enforcement activity may be coming to a close. Although the overall volume of civil audits and criminal investigations has declined in recent years, last year's Inflation Reduction Act, signed into law by President Biden on August 16, 2022, may reverse this trend. The Inflation Reduction Act allocates \$79.6 billion to the IRS over the next 10 years, with more than half of the money going to enforcement. This law aims to supplement, not replace, the IRS's normal annual appropriations. Stay tuned—only time will tell how these additional funds will impact the volume and focus of IRS's criminal financial investigations.

The IRS remains a significant player in white collar crime enforcement. IRS Criminal Investigation ("IRS-CI") is the federal agency responsible for investigating and recommending prosecution of criminal tax violations and other related financial crimes to the Department of Justice. It is the only agency that dedicates one-hundred percent of its time to financial investigations and the only agency with authority to investigate criminal violations of the Internal Revenue Code. According to the IRS-CI's 2022 annual report ("2022 Annual Report"),^[1] this past year IRS-CI spent 71.7% of its time investigating tax-specific crimes, 15.2% of its time investigating non-tax financial crimes such as money laundering ("tax fraud in progress"), and 11.6% of its time on narcotics-related financial cases through participation in the Organized Crime Drug Enforcement Task Force.

IRS-CI Chief Jim Lee, a veteran of the organization, continues to head the division. He touts the agency's 90% conviction rate, warning crowds around the

country that "if a CI special agent has you in their crosshairs, there is a good chance you are going to jail." Indeed, the incarceration rate for those sentenced in 2022 is 77%, with an average of 42 months to each sentence.

IRS-CI specifically emphasized the following areas of focus in 2022:

Cryptocurrency and Cybercrimes

IRS-CI has been investing in its cybercrime program since 2015, and that investment shows no signs of slowing. Calling it a "strategic realignment," IRS-CI has focused on building internal capabilities to address cybercrime in recognition of the growing role digital assets play in the global economy and the unique risks they present. In FY 2021, the agency created the Office of Cyber and Forensic Services ("CFS") to bring together digital asset investigation, cybercrime investigation, digital forensics, and physical forensics under one roof. The CFS supports criminal investigations agency-wide and, specifically, the Washington, D.C. and Los Angeles-based Cyber Crimes Units, which spearhead investigations into "the highest impact cases" of potential criminal activity involving digital assets. This year, IRS-CI plans to establish the Advanced Collaboration and Data Center, previously slated for completion last year, to provide centralized access to data and resources to effectively support investigations in challenging areas such as the dark web, cryptocurrency, and social media and other open-source platforms. This past year, IRS-CI's cybercrime efforts continued to focus on cryptocurrency. In fact, all three of the cybercrime cases highlighted in the 2022 Annual Report involve the nefarious use of cryptocurrency, including the April 2022 seizure of Hydra, a darknet marketplace

that conducted transactions using cryptocurrency. Looking ahead, IRS-CI identified decentralized finance, peer-to-peer payments, and anonymity-enhanced cryptocurrencies as “evolving” threats that the agency is working to address.

Sanctions-Related Investigations

As we noted last year, IRS-CI has a strong international presence, with attachés of the agency in 11 countries and partnerships around the world. In 2022, international activity took center stage, with an increase in investigations into financial crime connected with sanctions on Russia and Russian individuals. IRS-CI participated in a multi-agency task force, Task Force KleptoCapture, which was established to locate sanctioned Russians and their assets. IRS-CI also relied on its international partnerships, including its leadership of the Joint Chiefs of Global Tax Enforcement (J5), to identify potential sanctions-evaders or sanctioned assets and to develop a global strategy to deter Russian’s aggression.

Beyond these areas at the cutting edge of IRS-CI’s efforts, traditional examinations and enforcement actions against high-income individuals and large companies are and will always be a focus for the IRS. With both tax and non-tax crimes, the number of investigations initiated by IRS-CI increased slightly in 2022, but IRS-CI recommended prosecution in slightly fewer cases than the year before. Given the time-lag in tax investigations in prosecutions, it is possible that tax enforcement is or will soon be on the rise, as IRS-CI and others have been projecting for years.

—

[1] See links to recent IRS annual Data Books [here](#), and IRS-CI Annual Reports [here](#).

HEALTH CARE ENFORCEMENT: REVIEW OF 2022 AND A LOOK AHEAD TO 2023

BY LYNN NEILS

FEBRUARY 21, 2023

Health care fraud enforcement remained a top priority at both the national and local levels in 2022 and we predict 2023 will be no different. This post details certain categories of health care fraud that regulators and government agencies have indicated will be a focus in this coming year as well as other expected trends. The key takeaways are the following:

- **Opioids**

Both federal and state governments were extremely active in opioid-related enforcement actions in 2022, as they have for many years now, and the Department of Justice (“DOJ”) announced its continued commitment to focus on individual medical professionals as part of this effort.

- **COVID-19**

Health care fraud in connection with COVID-19 relief funding remains a focus of DOJ, which announced in September that it was creating three new Strike Force teams dedicated to these types of matters.

- **Telehealth**

Regulators and DOJ have demonstrated that it will continue to focus on telehealth services—a space that is still new and found to be susceptible to fraud and abuse.

- **Data Analytics**

Data analytics remains central to the investigation and prosecution of health care fraud and will likely only grow in its importance in the coming year.

- **False Claims Act (“FCA”)**

The FCA is an important tool for both government enforcement and private relator actions in the

health care fraud realm. The Supreme Court is set to hear important questions related to the FCA, which may transform how the FCA is used in future enforcement actions.

Opioids

Opioid enforcement actions were a core focus for both DOJ and state enforcement agencies this past year. Enforcement has not only focused on companies, but also on individuals. Earlier in 2022, DOJ announced the “2022 Opioid Enforcement Action.” This action included charges in eight federal districts against 14 individuals, 12 of whom were medical professionals, and related to unlawful distribution of prescription opioids. [In announcing this action](#), DOJ emphasized the work it has done so far to combat the opioid crisis but made clear that “[its] work is far from done.”

Indeed, similar enforcement actions have continued across the country. In October 2022, a doctor in Maine was arrested on criminal charges for allegedly prescribing opioids without a medical purpose. And, at the beginning of this month, nine individuals were arrested in Texas for their roles in a “pill-mill pharmacy” scheme, selling opioids on the black market. DOJ has also demonstrated its commitment to this effort by [creating](#) a New England Prescription Opioid Strike Force this past year with a focus on investigating individual medical professionals.

Accordingly, aggressive enforcement of opioid-related fraud is likely to continue in 2023.

COVID-19

Although President Biden recently [announced](#) that he would end the official national emergency declaration for COVID-19 in May 2023, which

will begin the decrease of distribution of federal COVID-19 relief money, enforcement actions related to COVID-19 are not necessarily set to slow down quite yet this year. 2022 saw a number of settlements in connection with COVID-19 funding and resources. DOJ has largely focused these efforts on borrowers under the Paycheck Protection Program (“PPP”), enacted to provide loans to assist small businesses in paying day-to-day business expenses during the pandemic. In just 2022, DOJ resolved 35 FCA matters tied to allegations that borrowers improperly received these loans and it recovered over \$6.8 million. DOJ also obtained its first-ever FCA settlement with a lender who improperly disbursed PPP funds. Settlements have further continued into the beginning of this year; for example, three companies recently settled FCA allegations relating to improper PPP loans, totaling over \$500,000.

In September, DOJ [announced](#) three new COVID-19 Fraud Strike Force Teams “to support, enhance, and continue” DOJ’s efforts to combat COVID-related fraud demonstrating that these types of actions are likely to continue through 2023.

Telehealth

The federal government greatly expanded the types of telehealth services that federal payors could cover at the start of the COVID-19 pandemic, and these services continue to be used at high volumes. Regulators and government enforcement agencies have accordingly scrutinized this new type of health care.

Last year, there was a nationwide DOJ [“Telemedicine Enforcement Action”](#) that alleged a healthcare fraud scheme utilizing telemedicine and involving more than \$1.2 billion in losses. There were charges in 13 federal districts against 36 defendants, including a telemedicine company executive. CMS also took administrative action against 52 providers involved in similar schemes. The schemes generally involved medical professionals making referrals for allegedly medically unnecessary cardiovascular genetic testing, cancer genetic testing, and durable medical equipment. For example, one case involved a clinical laboratory charged with paying kickbacks to telemedicine companies to induce those companies’ physicians to order the clinical laboratory’s tests. Of note, in announcing this enforcement action, DOJ declared its view that “fraudulent cardiovascular

genetic testing[] [is] a burgeoning scheme.” This multi-district enforcement action follows a similarly large enforcement action in 2021, where DOJ announced charges against 138 defendants across 31 federal districts in connection with fraud schemes, many of which related to telemedicine. DOJ will thus likely continue its focus on telemedicine schemes in 2023.

Recently, the U.S. Department of Health and Human Services, Office of Inspector General (“OIG”) promulgated its report [“Insights of Telehealth Use and Program Integrity Risks Across Selected Health Care Programs During the Pandemic.”](#) A portion of the report was dedicated to “program integrity risks associated with billing for telehealth services,” which it found included upcoding, duplicate billing for the same service, billing for services that were never actually provided, billing for services that were not medically necessary or that were inappropriate for telehealth, and ordering durable medical equipment, supplies, or laboratory tests. As one example, OIG found upcoding (i.e., billing for the highest, most expensive level of telehealth services even though those services were not provided) where one provider treated an individual consistently for 45-50 minute sessions but billed for 60 minutes of psychotherapy each time. Companies should be aware of these risks and update compliance programs accordingly.

Data Analytics

A constant theme across various instances of health care enforcement is DOJ’s use of data analytics. For example, in battling the opioid crisis, DOJ has created numerous strike force teams. DOJ has [explained](#) that, in addition to traditional investigative techniques, these teams “use advanced data analysis techniques to identify aberrant billing levels in health care fraud ‘hot spots.’” DOJ, in fact, chose to convene its most recent strike force team in New England because, as Assistant AG Polite [stated](#), he “asked [the] Fraud Section to identify the data, study the data, and identify where [DOJ] should [based on identified risks from that data] replicate [the] strike force model . . . [and] the New England area was the clear answer.” DOJ has also created three COVID-19 Fraud Strike Force Teams, which it [announced](#) are “designed to accelerate the process of turning data analytics into criminal investigations.”

In the telehealth sphere, the OIG noted in its above-referenced report that federal programs use data analysis to oversee telehealth medicine (e.g., “data analysis identifies concerning billing patterns in claims data”). And the report urges federal programs to go further in the monitoring and oversight of telehealth services, including targeted data analysis of the risks identified in the report and mentioned above.

In general, as AG Merrick Garland recognized in a [speech](#) last year, an “important force-multiplier is data analytics” and DOJ is only continuing to strengthen its “ability to bring data-driven corporate crime cases nationwide.” DOJ, and other agencies, are likely to continue relying more and more on data analytics to investigate and prosecute companies and individuals for health care fraud.

FCA

The FCA is consistently a powerful tool used in the fight against health care fraud. This is especially due to the ability for private individuals—relators—to bring *qui tam* actions under the FCA. *Qui tam* actions are approximately 75% of the new health care FCA matters that arose in 2022. Further, almost 95% of the value of the settlements and judgments recovered for health care FCA matters last year came from *qui tam* actions.

Notably, there are some thorny issues that remain as a source of contention within the FCA world that are being litigated at the Supreme Court this coming year. In one of these cases, *United States, ex rel. Polansky v. Executive Health Resources, Inc.*, the Supreme Court will decide whether the government has authority to dismiss a FCA suit after initially declining to intervene in the action. In a second set of cases, *United States ex rel. Schutte v. SuperValu Inc.* and *United States ex rel. Proctor v. Safeway, Inc.*, the Supreme Court will clarify the scienter element of the FCA. (For a more detailed discussion of the FCA and these cases, see our recent post [here](#)). Depending on how these issues resolve, FCA cases may be harder to successfully progress through the courts and the number of actions could begin to subside. Nonetheless, for now, the FCA—and *qui tam* matters more particularly—will continue to serve a central role in health care fraud enforcement.

SCRUTINY FOR THE PRIVATE SECTOR WILL COME FROM BOTH SIDES OF THE AISLE IN THE 118TH CONGRESS

BY VERONICA RENZI, YONI BARD, PATRICK BRENNAN

FEBRUARY 22, 2023

Key Takeaways

- With Republicans gaining control of the House, the party has plans to investigate both areas of focus from past Congresses, such as federal support for clean energy companies, and new areas, such as ESG practices.
- Certain areas of interest—especially China, large technology companies, and health care costs—will draw scrutiny from both parties and likely will continue in future Congresses.
- Some investigations that primarily focus on government actors, like scrutiny of the COVID-19 response or federal law enforcement investigations, are likely to draw in private sector entities as well.

Last year, as we laid out the [landscape for congressional investigations](#) in 2022, we noted that Democratic control of both the House and Senate enabled members of Congress to use investigations of the private sector and government entities to drive their party's legislative agenda. In 2023, as the 118th Congress opens with a Republican-controlled House and Democratic Senate, companies can now expect potential scrutiny from Congress on even more fronts than before.

With a divided government and significant legislation having passed in 2022—such as the Inflation Reduction Act (IRA) provisions on drug pricing and climate change and the CHIPS and Science Act's investment in the U.S. technology industrial base—Congress may find even more reason to focus on

investigations rather than major legislation in 2023.

Leadership in each party has already identified numerous areas of investigative interest that may lead to requests or subpoenas for information and testimony from private sector entities, including U.S. companies' relationship with China; the COVID-19 pandemic; turbulence in cryptocurrency markets; firms' use of environmental, social, and governance (ESG) practices; federal support for clean energy companies; and health care and prescription drug costs.

Investigating COVID-19

In the House rules package released in early January, House Republicans established a Select Subcommittee on the Coronavirus Pandemic that will fall under the House Oversight and Government Reform Committee, following the Democratic House's ambitious COVID-19 oversight committee in the 117th Congress. Like its predecessor, the new House committee looks likely to focus primarily on investigations of government entities, including federal funding of gain-of-function research, uses of COVID-19 relief funds [by state and local governments](#), and governments' pandemic response on issues like school closures.

However, the panel is also slated to investigate the development of COVID-19 vaccines and therapeutics, with Rep. James Comer (R-KY), chair of the House Oversight Committee, [stating](#) that he is planning to "talk to researchers" involved in the development of vaccines, including employees at the National Institutes of Health. Companies involved in the public-private vaccine and therapeutic development efforts, as well as companies that may have interests in oversight of federal scientific research funding,

will want to stay tuned to Republicans' COVID-19 oversight work.

Surveilling the China-U.S. Relationship

The House rules package also establishes a Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, chaired by Rep. Mike Gallagher (R-WI). Although Gallagher has primarily focused on national security issues in Congress, Republicans have indicated that they see China-related national security concerns as encompassing a wide array of economic and business relationships between U.S. firms and China. Republicans have identified a number of particular areas where they expect to use oversight to push back on what they have [called](#) China's "coordinated whole-of-society strategy to undermine American leadership and American sovereignty":

- Chinese foreign direct investment in the U.S., including [real estate](#), and [U.S. firms' investments](#) in China.
- American supply chains' dependence on China, an issue that also attracted substantial interest in the previous [Congress](#).
- Chinese companies' treatment of U.S. intellectual property, an investigation that U.S. private-sector stakeholders such as the [National Association of Manufacturers](#) and the [U.S. Chamber of Commerce](#) have identified as a positive opportunity for exposing Chinese practices and challenges facing U.S. companies.
- Potential human rights abuses in China, which, under the [Uyghur Forced Labor Protection Act](#), have now become a significant legal issue for U.S. firms.
- Chinese companies' practices in the U.S., with TikTok's policies around content moderation and U.S. citizens' personal data already having received detailed scrutiny from [Gallagher](#) and others.

As the above list makes clear, U.S. firms with significant exposure to China in a variety of ways—from having manufacturing facilities or other activities located in China to joint ventures, investment agreements, and other relationships—could potentially have interests at stake in the Select Committee's work.

A select committee like this one lasts for the duration of the rules established for the 118th Congress, but it can also be continued into a future Congress under a future rules package. The House Select Committee on the Climate Crisis, for instance, lasted through the 116th and 117th Congresses. While Republicans opted not to continue the climate committee, a committee focusing on China-related oversight may be more likely to endure in a future Congress. In other words: Don't just expect the growing oversight interest on China issues to float away like a weather balloon.

The Financial Industry: Examining ESG and Cracking Down on Crypto

As we noted in our review of congressional investigations last year, new trends in the financial sector are always popular targets for congressional oversight—especially when they grab headlines, as turbulence in cryptocurrency markets did throughout 2022.

Last year, we noted Congress's interest in a range of cryptocurrency issues, with particular focus on cryptocurrency practices that may have a greater effect on the broader financial system, such as "stablecoins" that are pegged to the price of a commodity or currency. In 2023, one particular focus will be cryptocurrency exchanges, with the Senate Banking Committee having launched an investigation of FTX's bankruptcy in December 2022. This interest is certain to continue in 2023, covering not just the practices of cryptocurrency exchanges but also their relationships with regulators. Such activity may also directly inform legislation on cryptocurrency regulation, with now-Chairman of the House Financial Services Committee Patrick McHenry (R-VA) saying that the FTX events demonstrate the need for Congress to create a clear regulatory framework for cryptocurrency.

While financial firms' use of environmental, social, and governance (ESG) principles may not generate as many exciting headlines as the cryptocurrency industry does, Republicans made it clear in recent years that they see ESG as a ripe area for investigation. The Securities and Exchange Commission's work on its 2022 proposed rules on climate disclosure will also be an oversight target, with a top Republican on the House Financial Services Committee promising "rigorous oversight of both regulators and private sector asset managers who

have politicized capital allocation.” ESG investigations may extend not only to companies that have touted their own ESG practices, but also firms that play a role in the dissemination or rating of practices throughout industries, such as proxy firms, accounting firms, and rating agencies.

Temperature Stays Elevated for Energy and Climate

In 2022, Democrats made investigations of oil and gas firms a high priority, using their oversight powers to build a case for legislation on energy and climate. Now, with the passage of the IRA’s major new programs to support green energy investments, as well as new programs created by the Infrastructure Investment and Jobs Act of 2021, Republicans see oversight of these programs as a top priority. This will include oversight of the Department of Energy’s Loan Programs Office and Office of Clean Energy Demonstrations, with one Republican member already saying that they view the dramatic expansion of such programs to be a potential “Solyndra on steroids” (referring to the bankruptcy of a solar firm that received a loan guarantee under the 2009 economic stimulus bill).

Republicans have also shown interest in investigating the Department of Energy’s management of the Strategic Petroleum Reserve during oil price spikes in 2021 and 2022, as well as dealings with foreign oil producers over pricing, which could sweep in private sector entities involved in those efforts. Although attention to energy and gas prices has abated somewhat, Democratic leadership has indicated that oil and gas companies remain a topic of significant interest for oversight, with Sen. Ron Wyden (D-OR) recently highlighting one oil company’s stock buyback and using it to draw attention to a proposal for a windfall tax on oil and gas profits.

Keeping an Eye on Health Care Costs

With the passage of the IRA in 2022, Democrats in Congress achieved a long-desired goal of overhauling how Medicare pays for prescription drugs. However, health care costs remain an area of vigorous interest, including hospital costs and drug-pricing issues that were not directly addressed by the IRA. Sen. Bernie Sanders (I-VT) has made no secret of his desire to investigate pharmaceutical companies and their pricing practices, promising a “very aggressive” oversight

strategy and framing such concerns in a recent Fox News op-ed as an area of bipartisan interest.

Pharmaceutical companies aren’t the only health care firms that will be attracting oversight in the new Congress. House Ways and Means Chairman Jason Smith (R-MO) has emphasized an interest in price transparency measures and highlighted hospitals’ level of compliance with the 2020 final rule on price transparency as a particular area for oversight.

Focusing on the Federal Government

The new Republican leadership in the House has also shown that it plans to devote significant oversight resources to investigations of the Biden Administration and federal agencies. This will include the work of the House Select Subcommittee on the Weaponization of the Federal Government’s investigations of federal law enforcement agencies, but also the Biden Administration’s COVID-19 response, implementation of the energy programs mentioned above, Biden family members’ personal business dealings, and more.

Despite their primary focus on the government, these investigations may interact with private sector firms as well. Rep. Jim Jordan (R-OH), chair of the subcommittee investigating the federal government, has indicated that he sees this effort as covering cooperation by technology firms with federal law enforcement, such as collaboration on content moderation decisions, and part of broader Republican efforts to investigate “Big Tech.”

Conclusion

Foley Hoag will continue to monitor the evolving work of congressional investigations throughout 2023, and we have outlined best practices for companies responding to such investigations. Companies concerned about potential congressional interest should bear in mind not only the above stated priorities of the 118th Congress, but also the shifting political priorities of the two parties in Congress, the Biden Administration’s actions, and media storylines that can fuel potential congressional interest in 2023 and beyond.

PREVIEWING SEC ENFORCEMENT IN 2023

BY CHRISTIAN GARCIA, SUSANNA CHI

FEBRUARY 23, 2023

Takeaways:

- The SEC's Division of Enforcement set record-highs in total money relief ordered and total civil penalties assessed in fiscal year 2022.
- The SEC will likely focus its enforcement efforts on securing the cryptocurrency industry's compliance with the registration requirements of the Securities Act of 1933 and ensuring statements made by investment advisers and issuers concerning their ESG-compliance are both truthful and not misleading.
- Amendments to the SEC's Whistleblower Program designed to incentivize a broader and larger range of whistleblower awards will continue to provide the Division of Enforcement with a pipeline of investigative leads.

The U.S. Securities and Exchange Commission ("SEC") continued its aggressive pursuit of investigations and enforcement actions in fiscal year 2022, setting records for the most money recovered and the most civil penalties assessed in a fiscal year. The SEC announced that its Division of Enforcement ("Enforcement") brought [760 total enforcement actions](#) in fiscal year 2022 (representing a 9% increase over fiscal year 2021), including 462 "stand alone" actions (enforcement actions excluding those brought against issuers for delinquent filings and "follow-on" administrative proceedings seeking bars against individuals), 129 actions against issuers for delinquent filings, and 169 "follow-on" administrative proceedings. Enforcement collected a record-setting \$6.439 billion (up from \$3.852 billion in fiscal year 2021),

including a record-high \$4.194 billion in civil penalties.

These metrics reinforce expectations that the SEC would take a more forceful regulatory stance under SEC Chairman Gary Gensler's and Enforcement Director Gurbir Grewal's leadership. We expect the SEC to continue to flex its regulatory muscles in fiscal year 2023, including by focusing on the priorities discussed below.

Crypto Likely to Headline Enforcement Efforts in 2023

Enforcement has advanced [Chairman Gensler's directives](#) to pursue unregistered sales of digital assets under the Securities Act of 1933 ("Securities Act"). Those enforcement actions included charges [against the founders of Forsage](#), an alleged "fraudulent crypto pyramid and Ponzi scheme" responsible for raising more than \$300 million; charges against [Payward Ventures, Inc. and Payward Trading Ltd.](#) for their alleged failure to register the offer and sale of their staking-as-a-service program; and charges against [Genesis Global Capital, LLC and Gemini Trust Company, LLC](#), for their alleged unregistered offer and sale of their Gemini Earn program, which provided investors with the opportunity to tender their crypto assets in exchange for a return. Of particular note, [Director Grewal has made clear](#) to the crypto space that Enforcement will continue to go after staking-as-a-service providers who fail to register their offerings, which generally provide investors with the ability to tender their crypto assets to a platform in exchange for a return.

The uptick and prominence of the SEC's enforcement actions in the crypto space follow the SEC's announcement that it was [bolstering Enforcement's Crypto Assets and Cyber Unit](#) (formerly known as

the Cyber Unit) with 20 additional positions, nearly doubling the unit's size. According to the SEC, those additional personnel will be responsible for protecting investors in crypto markets, and will be specifically focusing on crypto asset offerings, crypto asset exchanges, crypto asset lending and staking products, decentralized finance platforms, non-fungible tokens, and stablecoins. Since its creation in 2017, the Cyber Unit has been responsible for commencing more than 80 enforcement actions relative to fraudulent and unregistered crypto offerings and has collected more than \$2 billion in monetary relief.

With the high profile bankruptcy filings of crypto companies in recent months, and the SEC's investment in the Crypto Assets and Cyber Unit last year, we expect the SEC's regulatory and enforcement efforts into the crypto space to take center stage in fiscal year 2023.

Enforcement Tackles ESG Fraud

The SEC has continued its enforcement efforts into investment advisers and issuers characterizing their investment strategies and offerings as environmental, social, and governance ("ESG")-compliant. Last year, the SEC charged [BNY Mellon Investment Adviser, Inc.](#) for certain statements it allegedly made about its ESG considerations in connection with mutual funds. Specifically, the SEC's order alleged that BNY represented or implied that all investments in those mutual funds had undergone an ESG-quality review, when several investments in those funds did not have an associated ESG-quality review score at the time of the investment. In addition, the SEC charged [publicly-traded Brazilian mining company Vale S.A.](#) for its claims about the safety of its dams prior to the January 2019 collapse of the Brumadinho dam. The SEC alleged that Vale misled local governments, communities, and investors about the safety of the Brumadinho dam through various ESG disclosures. With ESG considerations taking increasing importance with retail investors, we expect the SEC to continue to probe ESG-related representations to ensure that the retail public is not being misled.

Individual Accountability Remains Priority

In November, the SEC [released its Strategic Plan](#) for the next four years, which emphasizes the agency's desire to hold individuals accountable for securities laws violations: "The SEC will continue to pursue misconduct wherever its staff find it and will use all of the tools in

its toolkit to deter those who might choose to violate the securities laws, including by holding bad actors – including responsible individuals – accountable." More than [two-thirds of enforcement actions](#) in fiscal year 2022 involved at least one individual respondent, a trend we expect to continue into 2023.

A number of the SEC's enforcement actions included high-profile individual respondents. For example, the SEC charged [the Boeing Company's former CEO](#) with making materially misleading public statements regarding the safety of Boeing's 737 MAX airplanes for his role in editing and approving company press releases and making other public statements following two airplane crashes. In another example, the SEC charged [Eagle Bancorp, Inc.'s former CEO and Chairman of the Board](#) with negligently making false and misleading public statements concerning certain related party loans Eagle Bancorp made to his family trusts. The SEC's pursuit of individuals in fiscal year 2022 extended beyond those circumstances where senior company leaders allegedly made false and misleading statements to the public, and included instances where the SEC charged [senior executives at public companies](#) for their failures to prevent misconduct at their firms, even where those executives themselves were not charged with the misconduct. These enforcement actions signal the SEC's intention to keep individual accountability at the heart of Enforcement's investigations.

SEC Enhances Whistleblower Program with Two Amendments

The Whistleblower Program received [12,300 whistleblower tips](#) in fiscal year 2022, representing the largest number of tips the Program has received in a fiscal year. Despite these record-setting figures, the Program dramatically decreased the amount of monetary awards provided to whistleblowers from 2021. The SEC awarded approximately [\\$229 million in 103 different awards](#) in 2022, less than half of the total amount of money provided in 2021 (\$564 million in 108 different awards). The largest awards in 2022 were a [\\$40 million award in October](#) and a [\\$37 million award in January](#), a notable decline from the largest awards in 2021 (\$110 million and \$114 million awards). Despite these drop-offs, the SEC continued to revamp the Program through multiple rule changes designed to incentivize more whistleblowers to come forward.

The SEC adopted [two amendments](#) to the Securities Exchange Act of 1934 in Rules 21F-3 and 21F-6, which became effective October 3, 2022. The amendments largely reverse controversial Trump-era policy changes to the Program that we discussed in our previous [installment](#). The two amendments (1) provide the SEC with the ability to award whistleblowers for information resulting in enforcement actions brought by other agencies or regulators where those alternative whistleblower programs contain more limited statutory award ranges, award caps, or discretionary awards, provided that the whistleblower waives any claim to the other program's award; and (2) affirmed the SEC's statutory authority to consider the dollar amount of a whistleblower award to increase, but not reduce, the award. Together, these amendments reinforce the SEC's commitment to incentivizing whistleblowers to report wrongdoing.

In addition to these policy changes, the SEC instituted enforcement actions against individuals and entities who allegedly retaliated against and obstructed would-be whistleblowers. For example, the SEC assessed a \$97,523 penalty against the [co-founder and former Chief Information Officer of NS8, Inc.](#) for allegedly retaliating against an employee-whistleblower by removing his access to the company's computer systems, surveilling his laptop activities, and prompting his termination. In another case, the SEC assessed a \$400,000 penalty against [The Brink's Company](#) for allegedly requiring employees to sign restrictive confidentiality agreements that prevented employees' communication with the SEC. These actions suggest the importance of the Program to the SEC's enforcement directives, and we expect the SEC to continue to rely upon the pipeline of information received by whistleblowers.

SEC's Reliance on Data Analytics Uncovers Insider Trading

The SEC increasingly relied on data analytics to ferret out potential securities law violations in 2022. In particular, Enforcement's Market Abuse Unit ("MAU"), which uses data analytics to detect suspicious trading patterns, contributed to significant insider trading enforcement actions within the last year. With assistance from the MAU, the SEC charged the [former chief information security officer of Lumentum](#)

[Holdings, Inc.](#) and others in connection with an alleged insider trading ring that generated more than \$5.2 million in illicit profits. The SEC alleged that the officer purchased securities of a target after learning about Lumentum's acquisition plans and tipped his friends about another target in advance of the information becoming public. The SEC was able to detect suspicious trading patterns using advanced data analytics, ultimately revealing the alleged insider trading, despite the fact that the officer used his wife's brokerage account and one of his friends siphoned the gains through a relative in India. In another case, the SEC charged an [investment banker and his friend](#) with insider trading after the MAU identified suspicious trading activity occurring before four acquisition announcements in 2017.

We expect the SEC to continue to rely on their advanced technology developments and the MAU to uncover difficult-to-detect insider trading. As expressed in its [Strategic Plan](#), the SEC aims to leverage emerging technologies such as machine learning and artificial intelligence to evolve and sharpen its data analytical tools in 2023 and beyond.

Enforcement Credits Cooperation with Recalibration of Penalties

Despite the SEC's announcement last year that it intended to take a [more rigid stance on cooperation credit](#) than it had during the Trump era, the SEC notably recalibrated penalties for companies that provided the SEC with meaningful cooperation. For example, the SEC charged [HeadSpin, Inc.](#) with fraud for the company's alleged inflation of certain financial metrics and fabrication of sales records, but did not impose a penalty on account of the company's extensive remedial actions. According to Director Grewal, the significant remedial actions taken by the company weighed against the imposition of a penalty. In another case, the SEC charged [Baxter International, Inc.](#) with engaging in improper intra-company foreign exchange transactions. But because of the company's remediation actions, including self-reporting; internal investigation; adoption of a new, GAAP-complaint foreign exchange rate convention; and recoupment of bonuses paid to the CEO and CFO, the SEC limited the penalty assessed against Baxter to \$18 million.

WILL STAKEHOLDER OBJECTIONS AND LEGAL UNCERTAINTY SLOW AN ESG REVOLUTION?

BY MATTHEW E. MILLER

FEBRUARY 24, 2023

According to the Securities & Exchange Commission, its proposed revisions to SEC regulations regarding climate change disclosures in May 2022 were intended to provide investors with consistent and reliable information regarding how climate change could impact their investment decisions. We have written previously about how these disclosure requirements affect investment advisers and about some of the key takeaways from climate-related disclosures under the new rule.

Many stakeholders and market participants have come out strongly against certain aspects of the proposed rules. We will revisit here the key points of the SEC's proposed rules (focusing on those drawing the most criticism), summarize the pushback the proposed rules have received, and consider where the SEC may go from here.

Revisiting Key Aspects of the SEC Proposal

In 2010, the SEC first adopted guidance describing how existing rules could require companies to disclose how climate change could impact their businesses. Specifically, the guidance focused on areas where climate change could trigger disclosure—the impact of climate change regulation and legislation on business, the impact of international accords, the indirect consequences of regulation or business trends, and the physical impacts of climate change. In short, the guidance directed companies to disclose ESG-related information based on whether such information was material as described in *TSC Industries v. Northway* (holding that a “fact is material if there is a substantial likelihood that a reasonable shareholder would consider it important in deciding how to vote”).

Last year, the SEC proposed new rules that would enhance climate-related disclosures for businesses. Should the new provisions go into effect, companies would be required to report climate-related risks that amount to 1% or higher of a total line item in a company's financial statements. As outlined in a press release, the provisions would also require registrants to disclose information about direct greenhouse gas (GHG) emissions and indirect emissions from purchased electricity as well as GHG emissions from upstream and downstream activities in its value chain if material or if the registrant has set a GHG emissions target. The proposal was open for public comment for 90 days following its proposal—originally ending in June 2022 but reopened until Nov. 1, 2022 after a technical issue impacted online comment submissions. In total, the SEC received more than 14,000 comments in response to the rule.

The Opposition

Companies have called on the SEC to reconsider its approach, citing the practical difficulties that would result from the proposal. Amazon.com Inc. noted that companies would need to essentially double their accounting efforts if the SEC required them to disclose lost revenues and avoided costs because of climate-related factors. Institutional investors, such as BlackRock, have commented that the 1% rule “would result in highly inaccurate disclosures and unduly burdensome compliance costs.”

Commissioner Hester Peirce has also criticized the proposed rules as unnecessary in light of existing rules requiring companies to disclose material risks. According to Commissioner Peirce, “rather than simply ticking off a preset checklist based on regulators’ prognostication of what should matter,

companies have to think about what is financially material in their unique circumstances” under those rules. As Bloomberg has noted, some companies object to the GHG reporting on the basis that they need “more flexibility” to reflect climate-related risks than such rules would allow.

Commissioner Mark T. Uyeda has suggested that the SEC’s usual “straightforward regulatory approach would treat ESG [a shorthand for Environmental, Social, and Governance issues] investing like any other investment strategy” and so makes ESG-specific regulations superfluous. In short, the SEC can bring enforcement actions against companies that fail to invest in a manner described to clients. Even without finalized rules, the SEC has brought ESG-related enforcement actions. For example, it charged BNY Mellon Investment Adviser, Inc. for representing that all investments in specific mutual funds had undergone ESG-quality review when several did not. The SEC also charged Vale S.A., a publicly-traded Brazilian mining company, for misleading investors and governments through its ESG disclosures regarding the safety of a dam it had constructed.

Beyond the fact that the SEC may already use its regulatory framework to pursue ESG-related fraud, Commissioner Uyeda described three problems with ESG-specific regulations. First, an objective definition of ESG is illusive and thus fails to provide standardized metrics for investors. Second, the SEC may be (undemocratically) putting a thumb on the scale in favor of certain ESG objectives. And third, asset managers may be pursuing ESG objectives without receiving such a mandate from their clients.

The Rationale

The SEC is considering “softening” rules mandating companies’ disclosure of the effects of climate change on its business in face of such opposition. So why might the SEC consider changing its climate change proposal?

First, as a matter of expedience, the SEC might alter its rules to demonstrate its own flexibility and to show that it’s listening, bolstering its chance of success in any court challenge once the final rules are adopted. Courts, such as the D.C. Circuit Court of Appeals in *Carlson v. Postal Regulatory Com’n*, have

noted that reasoned decision-making includes an agency’s response to public comments challenging its proposed rules. And the SEC may recognize that it could still achieve the majority of its climate change disclosure goals notwithstanding revisions around the edges of its proposal. Alex Martin, a senior policy climate analyst for Americans for Financial Reform has asserted that SEC could forego the 1% threshold rule and still achieve the majority of its disclosure goals where “other proposed changes to companies’ financial statements are more important, such as a requirement that companies to disclose the assumptions they use to make forward-looking estimates regarding, for instance, the profitability of fossil-fuel assets.”

Second, the SEC must have in mind recent successful legal challenges to agency authority. For example, in *NFIB v. OSHA*, the National Federation of Independent Business (NFIB) challenged OSHA’s promulgated rule requiring employers with at least 100 employees to require workers to receive the COVID-19 vaccine or wear a mask and be subject to weekly testing. The Supreme Court stayed OSHA’s vaccine mandate on the basis that the challengers were likely to prevail because the agency had exceeded its statutory authority. The Court noted that Congress had created OSHA to set workplace safety standards and that the rule at issue went beyond such authorization to essentially create “broad public health measures.”

West Virginia v. EPA placed another limit on agency authority. West Virginia and other states challenged the EPA’s authority to broadly regulate GHG emissions via the Clean Power Plan (repealed by the Trump administration which had its replacement, the Affordable Clean Energy Rule, vacated by the D.C. Circuit). The Supreme Court held that the EPA did not have the requisite authority to regulate GHG emissions under a generation shifting approach as outlined in the Clean Power Plan. The *West Virginia Court* made plain that because the EPA “assert[ed] highly consequential power beyond what Congress could reasonably be understood to have granted,” the agency needs clear congressional authorization to cap carbon emissions as outlined in the Clean Power Plan.

Given the Supreme Court's willingness to circumscribe an agency's authority to regulate beyond its mandate, the SEC may take a more cautious approach to avoid serious challenges that could result in courts curtailing the agency's authority.

Final Thoughts

The fate of the SEC's proposed rules on climate change disclosures remains unclear. Given the nature and amount of pushback the SEC has received, and the current legal environment of hostility to agency action that strays beyond the bounds of clearly proscribed authority from Congress, it seems likely the SEC may soften its proposals in the near future.

ANDREA CAMPBELL'S FIRST MONTH IN OFFICE: A REVIEW OF THE ATTORNEY GENERAL'S PRIORITIES

BY JEREMY W. MEISINGER, ROSIE LORING, RACHEL KERNER

FEBRUARY 27, 2023

2023 promises historic change for the Office of the Massachusetts Attorney General with Andrea Campbell sworn in as the new Attorney General earlier this year. Andrea Campbell ran a campaign on the idea that the Attorney General's office is uniquely suited to help in uplifting the underrepresented and her first month in office has signaled she intends to prioritize those groups. In her [inaugural address](#) on January 18, 2023, she outlined her priorities for her first term focusing on the theme that had come to define her candidacy. Her historic inauguration speech focused on how she will hold the powerful accountable, create economic prosperity and stability for families, prioritize the mental health and well-being of young people and bring the community into that work to make the office more accessible to people across Massachusetts regardless of income, language, zip code or ability.

This post previews what we can expect in the coming year under the Office's new direction, namely a renewed focus on big topics like elder care; reproductive justice, gun safety, and access to education as well as a continued focus on the opioid crisis, labor violations, and healthcare.

The Elder Justice and Reproductive Justice Units

While campaigning, Attorney General Campbell vowed to form the Elder Justice Unit and Reproductive Justice Unit. Her vision was for these units to use the tools of the Office to protect Massachusetts elders from hardship caused by unequal access to health care, deceptive business practices, and fraud and to protect and expand the right to access safe and legal abortion and

reproductive care throughout the Commonwealth.

On her first day in office, Attorney General Campbell reiterated those vows^[1] and she has stayed true to her promise, already launching a reproductive-focused hotline – a free and confidential resource to connect Massachusetts-based health care providers, helpers, and patients obtaining care in Massachusetts with free legal advice and resources about abortion access and care.^[2] We expect a similar focus on Elder Justice is not far behind.

Gun Safety

Gun safety has been a prominent focus in Attorney General Campbell's first month in office. In less than a month in the Office, Attorney General Campbell has filed back-to-back briefs in support of common sense gun laws in Massachusetts.^[3] The first brief, filed in the First Circuit Court of Appeals, argues that Massachusetts handgun safety regulations do not violate the second amendment.^[4] The second brief, filed in the District of Massachusetts opposes a request for temporary injunction for a law that would ban the sale and possession of assault weapons and large-capacity magazines.^[5] The Massachusetts Attorney General also signed on to support gun laws in New York, joining a multistate coalition of 18 attorneys general in filing an amicus brief in support of New York's law prohibiting the carrying of firearms in places of worship and religious observation.^[6]

Attorney General Campbell has further signaled that she will be proactive in gun safety legislation. Most recently, she signed on to support Massachusetts state legislation to strengthen laws prohibiting the purchase, possession and use of silencers by amending the definition to mirror federal law.

Gun safety was a major issue in Attorney General Campbell's campaign and it is likely to remain a top priority as she begins her term in office.

Access to Education

Attorney General Campbell's campaign promised to "fight to ensure that all students have access to high-quality public education regardless of geography or income."^[7] Her first days in office show execution on that promise. Indeed, Attorney General Campbell has already taken significant steps toward ensuring access to education, marking herself a leader in this sphere by announcing earlier this month that she would co-lead a coalition in support of a federal proposal to create a more affordable repayment plan for student loan borrowers. The coalition of 24 state attorneys general has since submitted comments to the Department of Education's Income-Driven Repayment Program. That plan enables borrowers to make payments based on income and family size and offers the possibility of loan forgiveness after 20 to 25 years of qualifying payments. Supporting this plan is consistent with Attorney General's Campbell's campaign promise to combat "predatory student loan practices that lead to burdensome debt and destroyed the credit ratings of individuals and families."^[8] Attorney General Campbell's steps toward access to education are taken on the heels of action by Massachusetts leadership earlier this year to secure a victory for student loan debt relief. On January 11, then Acting Massachusetts Attorney General Dewar led a group of 22 attorneys general in filing an amicus brief in support of the Biden administration's targeted cancellation of student loan debt to address the continuing effects of COVID.

Opioid Crisis, Labor Violations, and Healthcare

Attorney General Campbell's first month in office also saw a recommitment to labor violations, healthcare fraud, and combating illegal drugs, issues that were prioritized by prior Massachusetts attorneys general and on which Campbell also ran on. For example, in the labor space, earlier this month, the Office issued eight citations against USA Management LLC, a Georgia company that operates pool repair and lifeguard services to clients in Massachusetts for labor violations.^[9] The Office also joined a coalition calling for the federal government to set standards to

occupational heat exposure to protect workers.^[10]

With respect to healthcare fraud, the Office announced a settlement with a Taunton-based Mental Health Center, settling allegations of that the company submitted false claims to MassHealth for services provided by improperly supervised clinicians. In its press release announcing the settlement, Attorney General Campbell not only announced the resolution, but also issued a statement about the urgent need to address the mental health and behavioral health crisis facing Massachusetts.^[11]

On illegal drugs, in January, the Attorney General's New England Fentanyl Strike Force recovered 522 grams of fentanyl and \$20,000 in cash. The press release announcing the success of the Strike Force further reiterated the Attorney General Office's commitment to combatting the opioid crisis in the Commonwealth.^[12]

Looking Forward

Looking forward, we can expect to see a continuation of the efforts we have already seen Attorney General Campbell's office prioritize, such as workers' rights, reproductive rights, elder care and mental health, gun safety and access to education. Given her now proven track record of making good on campaign promises, onlookers should be on the lookout for Attorney General Campbell's office to take action on other issues she stressed on the campaign trail such as protecting immigrant communities and the LGBTQ communities through the use of anti-discrimination and civil rights laws, prioritizing the environment and combatting climate change through actions aimed at industries which historically contributed to these problems, protecting consumers against unfair and deceptive practices in developing industries including app-based services, and promoting affordable housing by investigating "digital redlining" by technology companies that sell discriminatory products. We will be sure to keep you updated on any developments in these areas.

[1] Press Release, Office of the Attorney General, Attorney General Andrea Joy Campbell Outlines Priorities in Historic Inaugural Address, <https://www.mass.gov/news/attorney-general-andrea-joy-campbell-outlines-priorities-in-historic-inaugural-address> (Jan. 18, 2023).

[2] Press Release, Office of the Attorney General, AG Campbell, Abortion Advocates and Law Firms Launch ‘Abortion Legal Hotline’ Amidst Unprecedented Legal Questions Following Dobbs Decision, <https://www.mass.gov/news/ag-campbell-abortion-advocates-and-law-firms-launch-abortion-legal-hotline-amidst-unprecedented-legal-questions-following-dobbs-decision> (Jan. 30, 2023)

[3] Press Release, Office of the Attorney General, AG Campbell Files Briefs in Support of Common Sense Gun Laws, <https://www.mass.gov/news/ag-campbell-files-briefs-in-support-of-common-sense-gun-laws> (Feb. 3, 2023).

[4] That case is *Granata v. Campbell*, No. 22-1478 (1st Cir).

[5] That case is *National Association for Gun Rights v. Campbell*, 22-cv-11431-FDS (D. Mass).

[6] Press Release, Office of the Attorney General, AG Andrea Joy Campbell Joins Coalition in Support of New York Law Banning Guns in Places of Worship, <https://www.mass.gov/news/ag-andrea-joy-campbell-joins-coalition-in-support-of-new-york-law-banning-guns-in-places-of-worship> (Jan. 27, 2023).

[7] On the Issues: Equal Access to Quality Education, Andrea Campbell: Attorney General, <https://www.andreacampbell.org/issues/education/>.

[8] *Id.*

[9] Press Release, Office of the Attorney General, AG’s Office Cites Georgia-Based Lifeguard Services Company for Labor Violations, Secures \$70,000 in Restitution for Workers, <https://www.mass.gov/news/ags-office-cites-georgia-based-lifeguard-services-company-for-labor-violations-secures-70000-in-restitution-for-workers> (Feb. 10, 2023).

[10] Press Release, Office of the Attorney General, AG Campbell Joins Coalition Calling for Emergency Federal Heat Exposure Standard to Protect Workers, <https://www.mass.gov/news/ag-campbell-joins-coalition-calling-for-emergency-federal-heat-exposure-standard-to-protect-workers> (Feb. 14, 2023).

[11] Press Release, Office of the Attorney General, Former Owners of Taunton-Based Mental Health Centers To Pay \$940,000 to Masshealth in Settlement, <https://www.mass.gov/news/former-owners-of-taunton-based-mental-health-centers-to-pay-940000-to-masshealth-in-settlement> (Feb. 13, 2023).

[12] Press Release, Office of the Attorney General, Boston Man Arrested and Charged in Fentanyl Takedown, <https://www.mass.gov/news/boston-man-arrested-and-charged-in-fentanyl-takedown/> (Jan. 27, 2023).



FEDERAL CRYPTOCURRENCY ENFORCEMENT IN 2023

BY CHRISTOPHER ESCOBEDO HART, YONI BARD, AMANDA S. COLEMAN

FEBRUARY 28, 2023

Key Takeaways:

- As we predicted in our March 2022 post, 2022 was a year of heavy cryptocurrency enforcement, with a spike in actions by the U.S. Securities and Exchange Commission (the “SEC”) and the U.S. Commodity Futures Trading Commission (the “CFTC”) against companies and individuals involved in cryptocurrency. It was also a year of major setbacks for the cryptocurrency industry, including the crash of the stablecoin TerraUSD (a cryptocurrency pegged to the value of the U.S. dollar that used an algorithm to control price fluctuation) and, shortly thereafter, the bankruptcy of the major cryptocurrency exchange FTX.
- The SEC and CFTC show no signs of slowing down their enforcement activities in 2023. But their approaches to enforcement have diverged, giving rise to what some see as a “good cop, bad cop” dichotomy: while the SEC continues to pursue perceived misconduct on a case-by-case basis against any crypto entity it believes offers a “security,” the CFTC is seeking express authority from Congress to expand its jurisdiction to fill regulatory gaps.
- The SEC’s active approach to crypto enforcement on a case-by-case basis, which recently included adding securities fraud charges against a defendant indicted for insider trading, has led to continued accusations that the agency is pursuing regulation by enforcement instead of promulgating clear rules that the industry can understand and follow.
- The tumultuous crypto events of 2022, combined with the heightened agency and executive action we have seen so far in 2023, could potentially spur Congress to act by passing one of the many cryptocurrency bills that have been introduced.

The SEC and the CFTC Continue to Dominate Crypto Enforcement

The SEC and CFTC each announced a record-breaking number of crypto enforcement actions in 2022. Jurisdiction over crypto activities, while messy, generally depends on whether the particular product or technology is a security (within the SEC’s remit), a derivative or commodity (the CFTC’s domain), or a currency (left to the Treasury Department). And while both the SEC and CFTC have been ramping up their enforcement, the SEC has expressed more confidence about the current scope of its enforcement authority over crypto assets. SEC Commissioner Gary Gensler believes most cryptocurrencies are securities that are already within the SEC’s purview, and has stated that crypto legislation should focus on stablecoins and granting the CFTC additional regulatory authority over digital assets that are not securities. CFTC Chairman Rostin Behnam agrees that the CFTC should fill the regulatory gap over non-security cryptocurrencies and that Congress should expressly grant it that authority.

The SEC

In 2022, the SEC announced 30 crypto-related enforcement actions (its highest number ever and a 50% increase from the 20 actions brought in 2021) and imposed \$242 million in monetary penalties. Further, in 2022, the SEC charged a total of 79 respondents in cryptocurrency enforcement actions,

of which 56 (71%) were individuals and 23 (29%) were firms. Gensler has repeatedly highlighted cryptocurrency as an enforcement priority, and he is now under pressure from Congress to take on crypto issues affecting investors following the bankruptcy of FTX. So we can expect to see heightened levels of crypto enforcement from the SEC in 2023.

On February 9, 2023, the SEC pushed the crypto exchange Kraken out of the business of providing interest to U.S. retail investors who loaned it cryptocurrency (a process known as staking). The SEC took the position that a staking product amounts to a securities offering, which should be registered with the SEC and should meet disclosure standards. Similar services are offered to U.S. customers from exchanges including Gemini, Binance.US, and Coinbase. But questions remain whether the SEC is more broadly targeting allstaking in the United States, how crypto companies can permissibly offer staking services, and whether the SEC will offer any guidance to companies that offer these services and do not want to be the SEC's next target.

Under Gensler, the SEC has been pursuing individuals at a higher rate. During the period of 2013-2020, on average, 20% of the agency's enforcement actions targeted individuals as opposed to entities. That rate rose to 35% in 2021 and reached 50% in 2022. The SEC scored a high-profile settlement in early 2023: on February 17, it announced that NBA champion and former Boston Celtics player Paul Pierce had agreed to pay more than \$1.4 million for allegedly making false and misleading statements about a cryptocurrency and sharing these statements on social media without disclosing his promotion fee.

The CFTC

Like the SEC, the CFTC's crypto enforcement numbers have been on the rise. In 2022, the CFTC announced 18 enforcement actions involving digital assets, up 73% from 11 actions in 2021 and representing more than 20% of all actions filed in 2022. In 2023, the CFTC will likely continue targeting platforms offering cryptocurrency derivatives based on theories that those companies have engaged in unlawful commodity transactions or failed to register with the CFTC.

On February 3, 2023, Chairman Behnam praised the

69 digital enforcement actions that had been brought by the CFTC to date during a speech to the American Bar Association. Behnam has been outspoken in his calls for greater crypto regulation, as well as his requests for congressional action to expand the CFTC's jurisdiction and increase its budget to allow it to play a larger role in crypto enforcement. According to Behnam, the CFTC wants to conduct more effective due diligence on businesses and grow its enforcement team.

Increased Action by Executive Agencies

While the SEC and the CFTC have been (and will likely remain) the two heavyweights in crypto enforcement, executive agencies have also been expanding their reach in this area. For example, the U.S. Department of the Treasury has continued to regulate the use of cryptocurrencies in international transactions. Recently, the Office of Foreign Asset Controls settled with crypto companies Bittrex and Kraken over alleged sanctions violations. Even the IRS is in mix, with its Criminal Investigation division hiring hundreds of new agents to work on digital assets and cybercrime.

The U.S. Department of Justice ("DOJ") remains committed to enforcing federal criminal laws against alleged violations related to cryptocurrency. One highlight in 2022 was the prosecution of the first-ever cryptocurrency insider trading case. Ishan Wahi, a former product manager at Coinbase Global, Inc. ("Coinbase"), pleaded guilty to two counts of conspiracy to commit wire fraud in connection with an alleged scheme to commit insider trading in cryptocurrency assets. His brother Nikhil Wahi had previously pleaded guilty to one count of conspiracy to commit wire fraud and was sentenced to 10 months in prison. While most insider trading cases are based on allegations of securities fraud, these indictments were based exclusively on wire fraud charges, which allowed DOJ to leave unaddressed the question of whether the crypto assets involved were securities.

But the SEC weighed in on that question, bringing a securities fraud action against the Wahi brothers in connection with the same conduct underlying the DOJ action. In its complaint, the SEC characterized the nine tokens the brothers traded as investment contracts, spurring CFTC Commissioner Caroline D. Pham to criticize the SEC's actions as a "striking example of 'regulation by enforcement.'" While the

Wahis maintain that the tokens are not securities under the law, the comment by Pham – herself a government official – highlights the view, held by some, that the SEC’s tactics are overly aggressive.

In late January 2023, the White House released a statement setting forth the administration’s roadmap for mitigating crypto risks, piggybacking on last year’s Executive Order on Ensuring Responsible Development of Digital Assets. The Biden administration highlighted the increase in enforcement by multiple agencies and called on Congress to take steps to expand regulators’ powers, and to strengthen transparency and disclosure requirements for cryptocurrency companies.

Signs of Emerging Legislation from Congress

It is possible that, in 2023, we may finally see congressional action on crypto. Notable legislation that has been introduced includes the bipartisan Lummis-Gillibrand Responsible Financial Innovation Act and the Digital Commodities Consumer Protection Act, both of which would give the CFTC the lead role in regulating crypto. In the Senate, lawmakers introduced the Digital Asset Anti-Money Laundering Act, which would apply current anti-money laundering and financing terrorism prevention methods to the crypto industry, and the Stablecoin Trust Act, which would establish a federal regulatory framework for payment stablecoins.

In the House, there’s the Keep Your Coins Act, legislation that would preserve an individual’s right to privacy when transacting with digital assets, and the Crypto Exchange Disclosure Act, a law that would mandate disclosure requirements for crypto exchanges. Finally, the Crypto Consumer Investor Protection Act, another House bill, would prohibit crypto exchanges from using customer funds in certain ways if the customer has not consented.

Both Republicans and Democrats have expressed a desire to increase scrutiny over the industry. If Congress remains resolved to act and the Biden administration continues to highlight the improvements needed in the crypto enforcement area, we could eventually see a more regulated and transparent industry, with increased market stability

and investor protection. Until then, crypto companies will have to look to past and current enforcement actions to see where the federal government is drawing the lines, and will need to continue exercising heightened levels of caution in this space.

FOREIGN CORRUPT PRACTICES ACT (FCPA) | 2022 YEAR IN REVIEW AND A LOOK AHEAD

BY SHRUTIH TEWARIE, LYNN NEILS, ANTHONY D. MIRENDA

APRIL 04, 2023

Key Takeaways

- DOJ continues to focus on corporate self-disclosure and remediation, individual accountability, and international cooperation on corruption matters.
- DOJ is putting new emphasis on the use of compensation system incentives and the threat of clawbacks to encourage compliance efforts by individual employees
- International efforts to improve whistleblower protections and increase beneficial ownership transparency continued to gain momentum

U.S. Policy Developments

Since the fall of 2022, DOJ has made several policy pronouncements in connection with its efforts to combat corporate crime. While it remains to be seen how these policies will ultimately affect DOJ's anti-corruption enforcement efforts, the policy pronouncements expand upon, and fill in the contours of, DOJ's prior policy commitments—particularly regarding the tangible benefits DOJ states are available to companies that voluntarily disclose misconduct.

DOJ's Updated Corporate Enforcement Memo

On September 22, 2022, Deputy Attorney General Lisa Monaco issued a memorandum providing additional guidance on how prosecutors should ensure individual and corporate accountability with the goal of promoting consistency in corporate criminal enforcement across DOJ. The memorandum

reiterates that individual accountability remains a top priority for DOJ, and that companies must disclose all relevant, non-privileged facts about individual misconduct in a timely manner to receive cooperation credit. The memorandum also emphasizes that prosecutors must consider the full range of a company's prior misconduct when determining the appropriate resolution. Not surprisingly, successive non-prosecution or deferred prosecution agreements for repeat corporate offenders are generally disfavored, especially where the matters at issue involve similar types of misconduct; the same personnel, officers, or executives; or the same entities. The memo also provides guidance on when compliance monitors are appropriate. Further, the memo notes that prosecutors may consider whether the company has compensation systems that encourage compliance and reporting, and whether the company has effective policies and procedures regarding the use of personal devices and third-party messaging platforms, in determining the terms of a resolution with DOJ.

Revisions to Corporate Enforcement Policy (CEP)

As we have written previously, Assistant Attorney General Kenneth Polite announced revisions to the CEP on January 17, 2023. The revisions expand upon DOJ's existing policy by more clearly identifying the tangible benefits available to companies that voluntarily self-disclose misconduct. The revisions provide that even when aggravating circumstances exist, such as the engagement of management personnel in the misconduct or where the corporation received significant profits from the misconduct, prosecutors may decline prosecution if: the

corporation voluntarily disclosed the misconduct immediately upon its awareness of such misconduct; the company had an effective compliance program in place; and the corporation provided “extraordinary” cooperation with DOJ. The revisions also provide that companies can receive tangible benefits for self-disclosure even in cases where DOJ has determined that a criminal resolution is warranted. Where a corporation has fully cooperated and appropriately remediated, DOJ may recommend a 50% to 75% reduction off of the low end of the sentencing guideline range (though generally not when the corporation is a “criminal recidivist”). Notably, the revisions specifically call out the benefits of self-disclosure in the mergers and acquisitions context. Where the acquiror uncovers misconduct of the target company, discloses such misconduct, rapidly remediates, and establishes an effective compliance program, there will be a presumption of declination.

Deputy AG’s Remarks on “Inspiring a Culture of Compliance” and Announcement of a Compensation Claw Back Pilot Program

Looking forward, on March 2, 2023, Deputy AG Lisa Monaco delivered remarks regarding DOJ’s ongoing efforts at combating corporate crime. Deputy AG Monaco announced the launch of the Pilot Program on Compensation Incentives and Clawbacks which consists of two parts. First, all corporate resolutions will now require the resolving company to develop compliance-promoting criteria within its compensation and bonus system. This feature has been encouraged in recent years; now mandatory, companies will have to be sure to incorporate this into their remediation plans in any negotiation with DOJ. Second, DOJ will provide fine reductions to companies who attempt to claw back compensation from corporate wrongdoers. In concept, resolving companies would pay applicable fines minus a reserved credit equaling the amount the company is attempting to get back. If the company succeeds, it will keep the clawback money and does not need to pay what it recovered. Further, if a company attempts to clawback money in good faith but is unsuccessful, it is still eligible for a fine reduction. In any specific situation, clawback efforts may face a number of practical challenges, including de-

confliction concerns between DOJ’s investigation and prosecution efforts on the one hand, and a company’s civil litigation efforts on the other. It will also require companies to carefully navigate the intersection with their indemnification obligations.

DOJ Issues Opinion Procedure Release Concerning Payments Made Under Duress

On January 21, 2022, DOJ issued a rare opinion procedure release – the first one since 2020, and only the second one since 2014. The specific facts at issue were unique – the Request sought guidance as to whether a payment to officials of Country A to release a captive ship and crew would trigger an enforcement action under the FCPA’s anti-bribery provisions. DOJ determined that the threat of imminent and serious physical harm to the captain and crew was sufficient reason to conclude that the payment would not be made with “corrupt intent.” In addition, DOJ considered that because the Requestor did not have any anticipated future business with Country A, it was not motivated by “obtaining or retaining business,” notwithstanding that the payment apparently would secure the release of the vessel as well. The Opinion is not binding on parties other than the Requestor and does not address whether the payment would violate other laws (such as those of Country A). This Opinion is noteworthy for two reasons. First, the Opinion shows that the procedure can be an effective mechanism to receive guidance from DOJ, and when exigent circumstances warrant, a company can obtain guidance quickly. In this instance, DOJ issued a preliminary opinion only one day after receiving the request given the circumstances. The Opinion also demonstrates DOJ’s willingness to consider true duress situations with care, and its focus on the “business purpose” motivating the payment in assessing liability under the FCPA. In this instance, the imminent safety threat, coupled with a practical assessment of the inability to rely on any other mechanism to secure the safety and freedom of the individuals in light of the circumstances presented by Country A, made the proposed payment “readily distinguishable from other situations in which a company is threatened with severe economic or financial consequences in the absence of a payment,” including situations where

payment is demanded “as a price for gaining entry into a market or to obtain a contract.” This Opinion helps expand on DOJ’s guidance regarding “true duress” situations, and provides some encouragement favoring swift and transparent consultation.

FCPA Enforcement Trends

Overall, the number of enforcement actions concluded in 2022 by DOJ and the SEC remained relatively flat compared to enforcement in 2021. Enforcement in 2021 and 2022 remained lower than the 10-year average beginning in 2013, and considerably lower than enforcement between 2016 and 2020. Looking forward, recognizing that FCPA investigations can take years to develop, we expect the number of enforcement resolutions to increase as the pipeline of investigations continues to fill.

Individual Enforcement

Despite identifying the prosecution of individual wrongdoers to be a top priority for years, the number of enforcement actions against individuals has declined since 2016. DOJ criminally charged 14 individuals in 2022, though only four were charged with substantive offenses under the FCPA (as opposed to related charges such as money laundering). Over the past several years, few individual prosecutions have resulted directly from corporate voluntary disclosures, but that trend may begin to change as cases in the pipeline begin to be brought.

United States v. Hoskins

As we have previously written, the Second Circuit’s decision in *United States v. Hoskins* could make it more difficult for DOJ to prosecute non-U.S. individuals under the FCPA. Lawrence Hoskins was charged and convicted for his alleged involvement in a scheme to bribe Indonesian government officials to secure a contract for a company’s (Alstom) U.S. subsidiary (Alstom Power, Inc.). The Second Circuit held that the government had failed to establish that Hoskins, a U.K. national, was sufficiently under the control of the U.S. subsidiary to have acted as its “agent” and so fell outside the reach of the FCPA. However, one judge on the panel issued a dissent which adopted a broader definition of agency, giving some indication that other courts may rule differently than the *Hoskins* majority.

United States v. Ng Chong Hwa

A jury convicted Roger Ng, a former Managing Director of The Goldman Sachs Group Inc., of conspiracy to commit bribery, circumventing internal accounting controls, and money laundering involving Malaysia’s state-owned investment fund. The case is noteworthy given it is one of the highest profile instances of a conviction for conspiracy to violate the internal accounting controls provision of the FCPA. That provision allows for prosecution of individuals who “knowingly circumvent or knowingly fail to implement a system of internal accounting controls.” Mr. Ng’s conviction may signal DOJ’s willingness to use the provision to go after corporate employees who they may not have enough evidence to charge with bribery, but who helped create or took advantage of an environment where internal controls systems were ineffective.

Business Entity Enforcement

While few, there were several notable enforcement actions in 2022 against business entities.

- United States v. UOP LLC d/b/a Honeywell UOP***
 UOP LLC agreed to pay more than \$160 million to resolve parallel investigations by authorities in both the U.S. and Brazil. Both DOJ and the SEC noted Honeywell’s remediation efforts as part of its rationale for providing offsets or credits of approximately \$40 million and \$39 million, respectively. Honeywell’s remediation efforts included strengthening its compliance program, terminating employees directly involved in the misconduct and demoting those employees with supervisory responsibilities over the offending employees, improving financial controls over third parties, and enhancing employee training regarding anti-corruption, controls, and other compliance issues.
- Stericycle***
 Stericycle, an international waste management company headquartered in Illinois, agreed to pay more than \$84 million to resolve parallel investigations by authorities in the U.S. and Brazil, and the SEC, related to bribery of public officials in Brazil, Mexico and Argentina. Stericycle entered into a 3 year Deferred Prosecution Agreement (“DPA”), and was

charged by criminal information with conspiracy to violate the anti-bribery and recordkeeping provisions of the FCPA. DOJ highlighted the nature, seriousness, and pervasiveness of the offense, coupled with Stericycle's failure to voluntarily and timely disclose the conduct that triggered the investigation, as key factors that were balanced against Stericycle's cooperation with the investigation, leading to the resolution. Significantly, despite Stericycle's extensive remedial measures, DOJ required imposition of an independent compliance monitor for two years because the company had not fully implemented or tested its enhanced compliance program.

- **ABB**

ABB, the Swiss based global technology company – an FCPA recidivist – agreed to enter into a three year DPA and to pay over \$315 million to resolve an FCPA investigation stemming from the bribery of a high ranking official at South Africa's state-owned energy company in connection with a power plant construction project. DOJ's resolution was in coordination with the SEC, which together imposed over \$147 million in penalties and disgorgement, and with authorities in South Africa, Switzerland and Germany. Both DOJ and the SEC announced that they would credit substantial portions of ABB's payments to those foreign jurisdictions against the amounts owed to the U.S. authorities. DOJ noted that the resolution balanced the seriousness of the misconduct and ABB's history of multiple prior FCPA violations against, among other factors, ABB's extraordinary cooperation and extensive remediation.

- **GOL Linhas Aereas Inteligentes S.A.**

GOL agreed to pay more than \$150 million (reduced to about \$45 million based on an assessment of GOL's inability to pay) to resolve civil and criminal DOJ, SEC and Brazilian investigations arising out of the payment of several million dollars in bribes to certain Brazilian legislators to secure the passage of favorable tax laws. GOL's extensive remediation efforts, including completely revamping its internal compliance program, coupled with its documented inability to pay, were key factors in the resolution.

- **Oracle Corporation**

Oracle agreed to pay more than \$23 million to resolve charges of violating the anti-bribery, books and records, and internal accounting provisions of the FCPA—paying \$8 million in disgorgement and a \$15 million penalty. The SEC accepted Oracle's offer of settlement partly on the basis that Oracle had cooperated by sharing facts from its own internal investigations, volunteered translations of key documents, and facilitated SEC requests to interview current and former employees of Oracle's foreign subsidiaries. Further, the SEC credited 12 distinct aspects of Oracle's remediation program, ranging from terminating employees involved in the misconduct to enhancing training and communications provided to employees and third parties regarding anti-corruption and internal controls.

In addition, the DOJ announced two declinations of prosecution in 2022, demonstrating its commitment to the aspects of its Corporate Enforcement Policy that provide some protection to a responsible acquirer in the M&A context and that reward voluntary disclosure and remediation.

- **Safran S.A. (Declination)**

DOJ determined that two Safran subsidiaries paid millions in bribes to a Chinese business consultant who was a relative of a senior Chinese government official to obtain government contracts. DOJ declined to prosecute Safran because the misconduct occurred before Safran acquired the subsidiaries, Safran detected the misconduct in post-acquisition diligence and promptly and voluntarily disclosed it, and Safran fully remediated, including agreeing to disgorge illicit profits from those contracts. DOJ credited Safran's willingness to resolve a parallel German investigation, and specifically noted with approval Safran's termination of one remaining employee who was involved in the misconduct and its withholding of deferred compensation owed to a former employee involved in the misconduct.

- **Jardine Lloyd Thompson (JLT) Group Holdings Ltd. (Declination)**

DOJ determined that a Jardine employee and agents of its subsidiary paid about \$3 million in

bribes to secure contracts with the Ecuadorian state-owned surety company which provided profits of over \$29 million. Jardine voluntarily disclosed the misconduct, fully cooperated in the investigation, separated from the involved employees and intermediaries, enhanced its compliance program and agreed to disgorge the entire \$29 million in profits. In light of this, DOJ declined to prosecute Jardine, and agreed to credit payments that it made to the UK's Serious Fraud Office to resolve a parallel investigation.

Anti-Corruption Efforts on the Global Stage

As can be seen from several of the DOJ's enforcement actions described above, anti-corruption enforcement is increasingly globalized, with law enforcement agencies cooperating on an international scale leading to substantial corporate resolutions. In addition, the international infrastructure supporting anti-corruption efforts continues to expand. Here are a few highlights:

France

Passed in March 2022 and effective October 2022, the French Whistleblower Protection Law (or "Loi Wasserman") as France's part in an EU-wide effort to expand whistleblower protections. The definition of "whistleblower" under French law changed, with the whistleblower now having to act "without direct financial consideration and in good faith" rather than "disinterestedly and in good faith." Importantly, the protection of whistleblowers now extends to individuals or entities that facilitated the whistleblower's reporting. The law now also allows whistleblowers to report wrongdoing to a "competent external authority or to the Defender of Rights [an agency charged with defending individual rights]" without having to file an internal report.

At this point, more than two-thirds of the members of the European Union have adopted whistleblower protections laws to implement the groundbreaking 2019 EU Directive on the protection of persons who report breaches of EU law. In the past few months, similar initiatives have become law in Belgium, Ireland, Finland, Greece, the Netherlands and Spain, among others. However, whistleblower protection efforts in two of the largest EU member states, Italy

and Germany, have been delayed, and those states should expect to face increasing pressure to move forward with adopting in the coming year.

United Kingdom

The Economic Crime (Transparency and Enforcement) Act of 2022

The Act was passed by the U.K. Parliament largely in response to the 2022 Russian invasion of Ukraine targeting Russian oligarchs and their assets in the UK. The Act requires any overseas entity owning land in the UK to identify their beneficial owners (according to specific requirements) and register them. The Act also strengthens the Unexplained Wealth Order (UWO) regime, which allows law enforcement to apply for a court order requiring entities and individuals to explain their interest in property and how they obtained it. The Act expands the category of persons subject to a UWO, to include responsible officers" (such as directors) of an entity that owns property. In addition, the Act allows for the granting of an UWO based upon a showing that there are "reasonable grounds for suspecting that the property has been obtained through unlawful conduct." Previously, a court needed to be satisfied that there are "reasonable grounds for suspecting that the known sources of someone's lawful income would be insufficient to obtain the property."

Increasing the ability to identify beneficial ownership has long been viewed as a critical tool in combatting corruption. Calls to increase transparency have continued to gain momentum since the 2016 "Panama Papers" revelations, with many international anti-corruption organizations such as Transparency International leading the chorus. In 2021 the Financial Action Task Force (FATF) issued comprehensive international standards to increase transparency. And in October 2022 the International Monetary Fund's Legal Department published a guide to assist countries in effectively implementing the FATF standards. Many countries are considering new laws in this area, and continued global developments will add to the due diligence and screening tools available for use in effective anti-corruption compliance programs.

Implementing Lessons Learned From a Review of the Serious Fraud Office's (SFO) Handling of the Unaoil Bribery Case

Former High Court judge Sir David Calvert-Smith was commissioned to review the SFO's previous efforts to investigate and prosecute the Unaoil bribery case. The review found a number of procedural and substantive shortcomings, and made 11 detailed recommendations. The SFO adopted the recommendations, and is now working to implement specific changes to its investigative process to provide greater supervision, particularly in the handling of sensitive cases, resolving internal conflicts, and providing an effective mechanism for raising internal concerns of misconduct.

NAVIGATING THE INTERNATIONAL TRADE & NATIONAL SECURITY LANDSCAPE 2023

BY SHRUTIH TEWARIE, ANTHONY D. MIRENDA, LUCIANO RACCO, NICK BERGARA, DANIEL ZALEZNICK

A Review of Recent Developments and What to Expect Going Forward

KEY TAKEAWAYS:

- Russia, China, and Iran will continue to be the focus of country-specific sanctions and export controls, but other hotspots around the world persist.
- The Biden administration will continue to focus on human rights, multi-lateral sanctions, and export controls coordinated with allies.
- Enforcement of sanctions and export control laws is expected to ramp up in 2023.

The centrality of international trade laws in the development and execution of U.S. foreign policy has never been more evident than in 2022. Companies that have not invested in international trade compliance programs are behind the curve and should do so with urgency as compliance and enforcement risks are set to materially increase in 2023. For a comprehensive review of these issues see the full publication [here](#).

COUNTRIES TO WATCH

Russian Federation & Belarus

Russia's invasion of Ukraine resulted in an unprecedented and rapid roll-out of new sanctions and export controls aiming to impose harsh economic costs on the Kremlin and its allies. Immediate, coordinated action from the United States, European Union and allies has been supplemented by a steady escalation of sanctions

and export controls restricting Russia's access to the global economy. These steps have involved almost every familiar policy in the sanctions toolkit, as well as some novel strategies developed and deployed for the first time.

Economic Sanctions

Some of the earliest steps taken by the U.S. in response to Russia's aggressive posturing towards Ukraine were to impose sanctions on regions of Ukraine that Russia recognized as independent, resembling those imposed by the Obama administration on the Crimea region of Ukraine back in 2014. These comprehensive regional sanctions were later supplemented by individual sanctions targeted on certain political and economic elites (so-called oligarchs) with close ties to President Vladimir Putin, senior Russian defense officials, as well as business leaders in the defense and aerospace industries.

U.S. sanctions were used to target the Russian financial sector, with numerous Russian financial institutions—both state and privately owned—added to the SDN List. OFAC also issued new directives drastically limiting financial transactions, bank accounts and payments in Russia. And many Russian financial institutions were cut-off from the SWIFT secure messaging system used by banks and other financial institutions to exchange information, such as details regarding money transfers. Without access to SWIFT, a financial institution is effectively denied access to the global economy.

In addition, the Biden administration released a series of executive orders that had the effect of prohibiting any new investment in the Russian Federation. The U.S. and EU banned the direct or indirect provision of certain business services (including accounting, trust and corporate formation, and business and management consulting) to Russia. The U.S. imposed substantial restrictions (subject to limited exceptions) on the provision of quantum computing services to any person located in Russia.

Export Controls

In addition to new sanctions, the United States implemented new export controls targeting Russia and Belarus. As with the sanctions regime, the new export restrictions targeted the defense, aerospace, and maritime sectors. Ultimately, the U.S. implemented a licensing requirement for all items on the Commerce Control List (“CCL”), which are destined for, reexported to, or transferred within Russia or Belarus that are subject to its jurisdiction, and implemented a new Russian Foreign Direct Product Rule restricting the export of a wide range of foreign-produced items. Additional restrictions targeted Russian military-end users, including a new Russian Military End-Users Foreign Direct Product Rule and an expansion of Military End User restrictions for nearly all items subject to the EAR.

In addition to imposing a ban on “luxury goods” exported to Russia or Belarus or to sanctioned oligarchs (irrespective of their location), the U.S. also broadened the scope of its licensing controls impacting certain goods, parts and equipment, and resources used in significant industry sectors, such as aviation, industrial and manufacturing activities, oil refining, and the production of chemical and biological agents. The UK and the EU have taken a similar approach, but the types of goods covered vary across the three jurisdictions.

To facilitate compliance and to monitor the effectiveness of the aforementioned rules, in June

2022, BIS, together with the Financial Crimes Enforcement Network (“FinCEN”), released a [joint alert](#) to financial institutions advising that they should apply increased due diligence to transactions that are more likely to enable the evasion of export controls. And export license applications related to products destined for Russia and Belarus are in most cases going to be reviewed by the U.S., EU and UK under a general policy of denial. Finally, the U.S. enacted regulations banning the exportation, re-exportation, sale, or supply of U.S. Dollar-denominated banknotes to any person located in Russia, including the government. The EU and UK have implemented comparable policies regarding the transfer of Euro and Sterling banknotes, respectively.

Russian Oil and Petroleum Price Caps

In December 2022, the G7 nations established a price cap on seaborne crude oil originating in Russia. In early February 2023, the G7 set two new price caps related to the maritime transport of other petroleum products that originate in Russia. All three price caps are governed by similar policies implemented by the U.S., the EU, and the UK. The U.S. price cap policy bans “the exportation, reexportation, sale, or supply” of the following services with respect to the maritime transport of covered petroleum products from the U.S. (or a U.S. person) to Russia, when the price per barrel is at or over the price cap: (1) trading/commodities brokering; (2) financing; (3) shipping; (4) insurance (including reinsurance and protection and indemnity); (5) flagging; and (6) customs brokering.

Notably, however, the U.S. (and the other jurisdictions) provides a safe harbor process whereby certain actors can avoid liability by meeting specific recordkeeping and attestation requirements. According to OFAC guidance, the level of diligence that different service providers have to perform depends upon the nature of the service provided and the provider’s access to price information. The EU & UK have implemented

similar price cap policies to the US and ongoing coordination among these jurisdictions is expected going forward as they all endeavor to stop Russia's ability to fund its war efforts against Ukraine.

Outlook for 2023

With no end in sight to the Russian invasion of Ukraine, we do not anticipate that the extensive sanctions implemented over the course of 2022 will unwind in the near-term. To the contrary, it is likely that the Biden administration will continue to issue new sanctions on Russian individuals with connections to the Putin regime and Russian entities in the industrial and financial sectors, as well as a focus on targeting sanctions evasion and increased coordination with multilateral partners.

More drastic steps remain available, but are unlikely except as an instrument of last resort. Unlike comprehensively sanctioned jurisdictions such as Cuba, Iran, North Korea, and Syria, there have been no signals that Russia will be designated as a state sponsor of terrorism in 2023.

For additional details, see the full publication [here](#).

China

Although overshadowed by the response to Russia's invasion of Ukraine, the Biden administration continued deploying export controls and, to a lesser extent, sanctions, throughout 2022 in an effort to slow China's development of technologies that the administration assesses threaten U.S. national security. In addition, as discussed further below, enforcement of the Uyghur Forced Labor Prevention Act has hit imports from China in certain industries.

Export Controls

In August 2022, without following a formal rulemaking process, BIS used a provision of its existing Military End Use / User ("MEU") Rule to notify parties (privately) that a license is required to export certain products, as a result of an "unacceptable risk of use in or diversion to a 'military end use' or a 'military end user.'" Parties

receiving these notices violate U.S. law if they export a product listed in the notice to one of the countries specified in the notice unless they have BIS authorization. License applications for these products are reviewed under a presumption of denial. This provision has reportedly been deployed by BIS to prevent multiple semiconductor companies from exporting particular types of integrated circuits ("ICs") and related technology, which is frequently used in advanced AI applications, to China (and Russia).

Along the same lines, in October 2022, BIS issued expansive export controls with respect to advanced computing integrated circuits ("ACICs"), computer products containing ACICs, and specific semiconductor manufacturing products destined for China. The U.S. government seems to be using these new export controls to prevent China from acquiring the technological resources (e.g., advanced computing software or supercomputers) it needs to develop sophisticated weaponry and computing that, among other things, could enable human rights abuses or pose a national security risk to the U.S.

In addition, the U.S. enacted two new foreign direct product ("FDP") rules (and revised an already existing one), extending the scope of U.S. export controls to specified foreign-produced goods connected to certain technology and software. While each FDP rule is different, the ones aimed at China are attempts to completely cut off its access to semiconductor manufacturing equipment, certain foreign-produced advanced ACICs, and products used in constructing and sustaining supercomputers.

In addition, BIS has placed significant restrictions on U.S. persons who are seeking to enable or engage in shipping or transferring certain items not controlled by the EAR, but that meet the parameters of certain ECCNs and may be used in the production, development, or servicing of ICs at semiconductor manufacturing facilities

located in China. BIS issued limited guidance regarding the application of the new rules.

Outlook for 2023

With no apparent off-ramp to cool tensions between the U.S. and China, and with fears that China may begin to supply military equipment to Russia for use in the war against Ukraine, it is clear that the U.S. will continue to use export controls, sanctions, and import restrictions to pressure China in 2023.

Iran

In 2022, the Biden administration continued to widen sanctions against Iran due to Iran's involvement in supplying arms to Russia for use in the war in Ukraine and human rights abuses. Sanctions targeted Iran's petrochemical industry, entities related to the production and transfer of Unmanned Aerial Vehicles ("UAVs"), and human rights-related sanctions in response to the Iranian regime's crackdown on protestors.

In addition, OFAC designated numerous persons who were involved in research, development, production, procurement, and shipment of Iranian UAVs and UAV components to Russia for its war against Ukraine, as well as firms that facilitated production or transfer of UAVs to Russia after Russia's use of UAVs to attack civilian infrastructure in Ukraine.

On September 13, 2022, Mahsa Amini, a 22-year-old woman, was arrested and detained by Iran's Morality Police for allegedly wearing a hijab improperly, and on September 16, she died under suspicious circumstances. Peaceful protests started in response, and the Iranian government violently suppressed those protests. In response, OFAC began designating Iranian persons who thwarted the protestors' freedom of expression. In addition, the US Department of Treasury issued Iran General License D-2 to support the free flow of information into Iran after the Iranian government cut off its citizens' access to the internet.

With little chance of a change in Iran's political regime, it seems highly likely that additional human rights-related sanctions will be imposed in 2023. Overall, we assess that sanctions against Iran will continue to increase in 2023, including by the EU, in response to deepening ties between Russia and Iran and political turmoil within Iran. The chances of a restoration of the JCPOA are virtually zero given geopolitical concerns and bipartisan opposition in the U.S. Congress.

Nicaragua

In 2022, the Biden administration continued to target officials of the Ortega-Murillo regime and executives in the gold sector. On October 24, 2022, President Biden signed Executive Order 14088, which expanded Treasury's authority to hold the Ortega-Murillo regime accountable for its continued attacks on Nicaraguan's freedom of expression and assembly, and provided OFAC with the authority to target certain entities or persons that operate or have operated in the gold sector of the Nicaraguan economy and any other sector identified by the Secretary of Treasury, in consultation with the Secretary of State. Lastly, the executive order allowed expanded sanctions that could be used to prohibit new U.S. investment in certain identified sectors in Nicaragua, the importation of certain products of Nicaraguan origin into the United States, or the exportation from the United States, or by United States person, wherever located, of certain items to Nicaragua.

In February 2023, the Ortega regime freed more than 200 political prisoners, which the U.S. State Department has described as a "constructive step towards addressing human rights abuses" in Nicaragua that could "open[] the door to further dialogue...." Whether this ultimately leads to an easing of U.S. sanctions remains to be seen. As of the time of this writing, sanctions on Nicaragua have not changed since the last round of sanctions that were imposed in October 2022.

Venezuela

In November 2022, Venezuela's government met with Venezuela's democratic opposition to resume negotiations. Both sides agreed to enact an estimated \$3 billion humanitarian relief program and discussed continuing efforts to proceed with fair and free elections in 2024. Not long after the parties reached agreement, OFAC announced Venezuela General License 41 ("GL 41"), which authorizes select transactions "related to the operation and management by Chevron Corporation and its joint venturers in Venezuela involving state-owned Petróleos de Venezuela, S.A. PdVSA." GL 41 significantly limits the U.S.'s pressure campaign against the Maduro regime for the first time since 2018, when essentially any dealings with a U.S. nexus that involved Venezuela's oil sector were prohibited.

Notwithstanding GL 41, all other Venezuela-related sanctions and SDN designations remain in place. However, depending on how negotiations proceed between Maduro's regime and the democratic opposition, the U.S. may look for additional ways to ease some Venezuelan sanctions to encourage further progress.

Export Controls

In addition to the targeted export controls imposed on the specific countries discussed above, both the Department of Commerce and Department of State imposed new, generally applicable, export controls.

U.S. Department of Commerce – General Export Control Developments

Section 1758 of the Export Control Reform Act of 2018 mandates that BIS establish export controls on "emerging and foundational technologies" ("Section 1758 Technologies"). In August 2022, BIS enacted an [interim rule](#) that imposes new export controls on four Section 1758 Technologies. These technologies are comprised of: two substrates of ultra-wide bandgap semiconductors (Gallium Oxide (Ga₂O₃) and diamond); Electronic Computer Aided Design software specially designed for

the development of integrated circuits with any Gate-All-Around Field-Effect Transistor structure; and pressure gain combustion technology for the production and development of gas turbine engine components or systems. In January 2023, Section 1758 Technologies restrictions were imposed on four marine toxins (brevetoxin, gonyautoxin, nodularin, and palytoxin) as well.

U.S. Department of State – General Export Control Developments

In March 2022, the U.S. Department of State's Directorate of Defense Trade Controls ("DDTC") announced it was conducting a multi-year comprehensive review and revision of the International Traffic in Arms Regulations ("ITAR"). DDTC took the first step when it amended the ITAR in September 2022 in an attempt to better organize the purposes and definitions of the regulations. While these were not substantive revisions, we anticipate those will come over the next few years.

In July 2022, DDTC initiated a pilot program for an Open General License ("OGL") process based on ITAR Section 126.9(b) and announced two OGLs that, unless otherwise noted, are in effect until July 31, 2023. One OGL provides for the reexport—to end users in the United Kingdom, Canada, or Australia that are pre-verified and approved—of unclassified defense articles. The other provides for the retransfer—to end users in the United Kingdom, Canada, or Australia that are pre-verified and approved—of unclassified defense articles.

In early December 2022, DDTC announced its [International Traffic in Arms Regulations Compliance Program Guidelines](#) (the "ITAR Guidelines"). The ITAR Guidelines outline DDTC's expectations for developing and maintaining an effective ITAR compliance program. These guidelines now contain a structure that is more consistent with that of the [Framework for OFAC Compliance Commitments](#) and BIS's [Export Compliance Guidelines](#). Finally, DDTC has released new guidance for those interested in soliciting authorizations with respect to defense service

exports by U.S. persons overseas. DDTC is likely to issue additional guidance and revisions to the ITAR in 2023.

CFIUS UPDATES

The Committee on Foreign Investment in the United States (“CFIUS”) had a busy year in 2022, and shows no sign of slowing down in 2023.

On August 2, CFIUS published an annual report analyzing its activities in 2021. In September, President Biden issued an executive order instructing the committee to consider particular national security risk factors, such as risk to supply chain resilience and security when reviewing covered transactions. And in October, the Department of Treasury released the first-ever [CFIUS Enforcement and Penalty Guidelines](#), providing important visibility into the committee’s enforcement approach by spelling out categories of acts or omissions that may lead to a penalty. Taken together, these three releases reinforce a continuation of trends seen over the past few years and suggest increased committee activity in the year to come. For 2023, high technology – including quantum computing – life sciences, and green energy technology will continue to be key areas of interest for CFIUS, as will critical technologies.

Transactions from China reviewed by CFIUS more than doubled in 2021. However, most reviewed transactions are expected to continue to involve foreign investors from allied countries, which pose less of a national security risk and are more likely to be approved by CFIUS without mitigation. We additionally expect CFIUS to continue to put non-notified/non-declared transactions under heightened scrutiny as the committee devotes resources to identifying such transactions through a variety of channels. The committee is expected to increase enforcement, especially for parties that fail to submit mandatory filings, fail to comply with CFIUS mitigation terms, or make inaccurate filings.

OTHER ISSUES TO WATCH:

Virtual Currency Sanctions Risks

Platforms providing services related to virtual currency emerged as a hotspot of OFAC enforcement activities in 2022. This increased emphasis has been a part of a whole-of-government approach to addressing risks associated with the use of virtual currencies, including sanctions evasion, but also money laundering, cybercrime, and financing of illegal activities. This increased scrutiny generated a number of enforcement actions against participants in the virtual currency industry in 2022. Given the nature of the services provided by cryptocurrency mixers, continued scrutiny by financial regulators and OFAC can be expected in 2023 and beyond. In addition, OFAC’s designations have included the addition of specific cryptocurrency wallet addresses to the SDN List. Users of virtual currency must avoid any transactions involving these addresses.

OFAC and FinCEN targeted enforcement against virtual currency exchanges, focusing on failure to prevent or detect transactions in violation of sanctions or anti-money laundering requirements, including the failure to implement IP address blocking on transactions. These actions indicate the overlapping risks associated with cryptocurrency exchanges as well as inter-agency coordination in addressing those risks.

It is now well-established that cryptocurrency exchanges and other virtual currency providers are highly vulnerable to charges of facilitating sanctions evasion without robust due diligence and know-your-customer protections. As the SEC, CFTC, and FinCEN continue enforcement actions, OFAC is likely to play a role in joint enforcement action or on its own where violations have a sanctions-evasion dimension.

Uyghur Forced Labor Prevention Act

On June 13, 2022, the U.S. Department of Homeland Security’s Customs and Border Protection agency

(“CBP”) published [guidance for importers](#) regarding compliance requirements under the Uyghur Forced Labor Prevention Act (“UFLPA”). The guidance provided by CBP describes the documentation and supply chain due diligence required to release a detained shipment. The guidance also highlighted enforcement priorities for CBP.

We expect CBP to continue to ramp up enforcement of the UFLPA. There are indications that that CBP may take enforcement action against the aluminum industry in China, and that cotton and apparel will continue to be a main focus of CBP’s enforcement of the UFLPA. CBP has also indicated that it would like to make its processes more transparent and it would not be surprising if CBP issued additional guidance this year on how companies can address imports blocked pursuant to Withhold-Release Orders (WROs), findings, and/or the UFLPA.

International Trade Enforcement Activities

Throughout 2022, the Department of Justice, BIS, the DDTC, FinCEN, and OFAC, among others, have been actively enforcing U.S. sanctions and export controls programs. As detailed below, they show no signs of letting up.

BIS Enforcement Guidance

BIS has modified its enforcement regulations so that BIS charging letters, some of which are already available on the agency’s website, can be made publicly available after they are issued. It has also issued a revised enforcement regime via a memorandum (the “[EAR Memo](#)”) that stresses four points: (1) substantially larger penalties; (2) more frequent use of non-monetary settlements for less egregious violations; (3) no longer allowing persons to settle a matter while neither admitting nor denying their actions (i.e., the party settling must admit the alleged conduct occurred); and (4) the institution of a 60-day “fast-track” review of voluntary self-disclosures involving technical (or minor) violations. BIS has also continued to develop its antiboycott rules which restrict

parties’ participation in foreign boycotts not approved by the U.S. Assistant Secretary Axelrod issued a separate [memorandum](#) outlining revised antiboycott enforcement policies, which, like the EAR Memo, underscored important enforcement priorities for BIS.

Academic Outreach Initiative

In June 2022, the Department of Commerce’s Office of Export Enforcement announced a new academic outreach initiative focused on preventing export controls violations by academic research institutions. The initiative signals a greater focus on investigation and enforcement by the U.S. government of export-controls related violations committed by universities and other academic research institutions, making important for such institutions to have robust export control compliance programs in place, including export control training for faculty and staff engaged in proprietary research.

For additional details, see the full publication [here](#).