January 31, 2023

White-Collar and Regulatory Enforcement:
What Mattered in 2022 and What to Expect in 2023

Introduction

Each year we try in this wrap-up memo to flag the main enforcement developments that companies should be alert to in the coming year and also to identify steps companies should be taking to prepare themselves in the event of a significant white-collar or regulatory enforcement inquiry. Because policy preferences (and politics) often shape these developments, the early days of any new administration in D.C. are frequently harder to read, and teasing apart mere rhetoric from concrete changes in enforcement priorities can be challenging. But now, two years into the Biden administration, we can see some clear themes emerging: Penalties are up—way up; investigations appear to be moving a bit faster; cryptoassets and cybersecurity have become heightened risk areas; government expectations for what constitutes full cooperation have been amped up; and many new disclosure demands across a wide range of corporate activities are coming on line. At the same time, however, several time-tested verities remain firmly in place, including the need to maintain strong internal accounting controls, provide comprehensive (and frequent) training, instill a genuinely ethics-oriented tone at the top, stay vigilant in detecting internal misconduct, and react swiftly in the event problems do arise by self-remediating and self-reporting when appropriate. A company that positions itself in this way optimizes its chances not only of securing the best possible resolution in the event of criminal or civil charges but also of forcefully resisting enforcement action where warranted.

Our general sense is that government investigators are becoming more adept at gauging whether a corporation's commitment to ethics and compliance is both genuine and commensurate with the risks its businesses entail. We also think the government is getting better at delineating when (and why) it is granting substantial credit for a robust compliance culture, effective remediation measures, and timely, comprehensive cooperation. In sum, as we look ahead, the rewards for getting compliance right are easier to see, while the costs of getting it wrong are increasing.

In the sections that follow, we describe how senior DOJ leadership delivered over the past year on its promise to provide companies with additional guidance regarding its corporate enforcement policies. Most notably, this past September, Deputy Attorney General Lisa Monaco promulgated a memo that further revised and made more transparent DOJ's policies concerning the evaluation of companies' voluntary self-disclosure of misconduct, cooperation efforts, compliance program and culture, and past history of misconduct. Since DAG Monaco's memo, other senior DOJ officials, through a series of public speeches, have built on these themes and emphasized white-collar enforcement as a key priority under the Biden administration. In January of this year, Criminal Division head Kenneth Polite announced revisions to the Corporate Enforcement Policy (CEP) that implement and refine aspects of DAG

Monaco's memo with a view to giving corporations yet more incentives to detect, report, and remediate misconduct, and engage proactively with DOJ.

The SEC has also made concrete its earlier talk of increasingly aggressive enforcement. For example, as we explain below, the Division of Enforcement "re-calibrated" its penalty-imposing ambitions and levied record high civil money penalties in 2022 for the articulated purposes of promoting deterrence and sending a signal to markets that penalties must not be seen as "another business expense." In several high-profile settlements, the SEC revived its policy of seeking admissions of wrongdoing. And recently adopted and proposed disclosure rules are likely to expose companies to new enforcement risks.

Finally, we cover below several of the key substantive areas that attracted the greatest attention in 2022, including developments in the cybersecurity, cryptoassets, antitrust enforcement, and cross-border arenas. We also review the active role played by state Attorneys General this year across a variety of sectors, most notably with respect to ESG policies, data privacy, and cybersecurity—a high level of enforcement activity that we expect to persist, and perhaps even expand, in 2023.

DOJ Developments

In October 2021, DAG Monaco issued a memo that heralded a return to Obama-era corporate criminal enforcement policies. In the memo and related remarks, the DAG and other DOJ officials championed a sweeping conception of corporate recidivism to stand as a barrier to leniency; threatened to withhold cooperation credit from companies that identified only those individuals *substantially* involved in misconduct; and encouraged prosecutors to dust off the corporate monitorship as a component of corporate criminal resolutions. The DAG also created an advisory group to help flesh out these policies. The hope expressed in our wrap-up memo last year was that, as events unfolded in 2022, DOJ would provide clarity and transparency about how it would exercise its discretion and grant credit for self-reporting and cooperation in the corporate context.

A year on, that hope has been realized to a significant degree. What is more, the refinements and clarifications DOJ has offered reflect more sensitivity to context and more flexibility than one might have predicted based on early declarations.

In September 2022, the DAG issued a follow-on memo reflecting the work of the DOJ advisory group. As we summarized at the time, some parts of that memo introduced welcome nuance and clarity. For example, the memo made it clear that before treating a company as a recidivist undeserving of leniency, a prosecutor should consider precisely what and who were involved in the prior conduct at issue, including whether the prior conduct was similar to the newly discovered conduct and whether the same personnel were involved, how long ago the prior misconduct happened, how that conduct was addressed (*i.e.*, whether there was a civil resolution, criminal charge, or some other disposition), whether the subject company operates in a highly regulated industry, and whether the prior conduct was that of an acquired entity that has since been integrated into a compliant entity. In other words, not all prior brushes with law enforcement should be weighted equally. Another heartening pronouncement was that a company that voluntarily self-discloses misconduct, cooperates fully, and adequately remediates

can avoid a guilty plea absent aggravating factors—and each DOJ component must adopt a written policy specifying what it considers an aggravating factor. Likewise, the memo clarified that a monitorship may not be warranted as part of a criminal resolution where the subject company has already implemented and tested an effective compliance program.

Further guidance on DOJ policy concerning corporate leniency—and declinations in particular—came in January 2023, with AAG Polite announcing a revised CEP that equips prosecutors with more carrots to reward self-disclosure, cooperation, and remediation. Under the new CEP, declination may be available even when certain aggravating factors are present—provided the company immediately self-discloses conduct caught by an "effective compliance program" and engages in "extraordinary" remediation and cooperation.

Our summary of the DAG's September 2022 memo applauded its transparency, because in our view the more concrete the guidance, the more effectively a well-managed company can direct its resources, address internal reports of misconduct, and respond constructively to regulatory inquiries—including by forcefully resisting enforcement action in appropriate cases. We likewise applaud the updating of the CEP to clarify that declination may be on the table even where there is an aggravating factor like executive management involvement in misconduct. But companies should make no mistake: the expectations embodied in DOJ's recent guidance are more demanding than ever for entities hoping for a favorable negotiated resolution. Companies wishing to gain credit for cooperation will be expected to produce documents and other records on a "timely" basis (emphasis in DOJ's September 2022 memo), prioritize production of—and direct prosecutors' attention to—the most relevant evidence from the most involved employees, and, where possible, resist reliance on foreign data privacy laws to avoid production of documents. As DAG Monaco's Principal Assistant, Marshall Miller, put it in a "Brooklyn-blunt" September 2022 speech, criminal charges and guilty pleas are now "on the main, everyday menu," and much is required of companies before DOJ will grant them leniency. If DOJ follows through on all of this tough talk, then companies should expect that simply cooperating in full will not necessarily result in a declination or a non-prosecution agreement. With the benefits of cooperation thus lessened and more difficult to secure, more companies may decide to run the risk of fighting in close cases.

Another principal takeaway from all of these DOJ pronouncements is that the heavy corporate lifting required for lenient treatment must start before the first subpoena arrives. Throughout 2022, DOJ officials have been emphasizing the need to create a compliant culture well in advance of regulatory scrutiny. They have urged companies to ensure their compliance programs set the right incentives for executives—including by using compensation and clawbacks to reward compliance and punish its opposite. DOJ has also now made it clear that companies hoping for cooperation credit should have effective policies for monitoring and preserving their employees' business-related communications over all platforms and media. Policies governing business-related texting, use of personal phones, and communications over ephemeral and encrypted messaging necessarily will vary depending on the company and the industry in which it operates. But a company hoping for leniency will want to ensure that it has a clear policy in place and is monitoring and enforcing compliance with that policy.

Because most DOJ investigations incubate for some time before their outcomes are publicized, it is too early to tell whether the Department's 2021 policy initiatives or their 2022 and early 2023 refinements will translate into a measurable increase in corporate criminal prosecutions and resolutions. Our prediction is that they will. No matter how intent prosecutors may be on rooting out, exposing, and deterring corporate misconduct, and however much support they may have from DOJ's leadership, resource constraints can be a significant limiter. The DAG's memos, the new CEP, and DOJ's related policy pronouncements are designed in large part to expand the prosecutor's resources by causing companies to deploy their own compliance tools and efforts in service of DOJ's mission. That marshaling of corporate resources to the government's advantage will likely yield more—and more significant—enforcement in this area.

SEC Developments

The current administration at the SEC arrived with promises of a more aggressive approach to enforcement. In the past year, we saw a variety of concrete results in keeping with that commitment, and we expect this emphasis on tougher enforcement to continue in the coming year. The Commission brought a total of 462 standalone enforcement actions in its fiscal year ended September 30, 2022. This was a 6.5% increase over the prior year, though still somewhat below each of the two years that preceded the onset of the pandemic. The case mix was broadly in line with historical patterns. Public company disclosure and accounting cases were 16% of the total, up slightly from 12% in 2021. Insider trading cases also increased somewhat, accounting for 9% of 2022's docket, compared to 6.5% in 2021. Securities offerings comprised 23% of the cases brought, but this category always includes a large number of unregistered offerings, Ponzi schemes, and similar matters—and relatively few cases involving offerings by public companies.

The administration's new approach was most strikingly illustrated in the civil money penalties the Commission extracted in 2022. Penalties ordered in SEC enforcement actions in 2022 totaled $4.194 billion—by far the most ever, and roughly three and four times the aggregate penalties levied in 2021 and 2020, respectively. In public remarks, SEC officials continue to emphasize their determination to increase penalties. Enforcement Director Gurbir Grewal's remarks at the Securities Enforcement Forum this past November are representative—he referred to the SEC's effort to "re-calibrate" penalties and expressed his desire to "get away from the idea that penalties are just another business expense." Unfortunately, rhetoric of this nature fails to recognize the strong compliance culture that exists in many companies. Such companies, when faced with SEC inquiries, should be prepared to make strong affirmative presentations about their commitment to ethical practices and strong controls.

The SEC has now also carried through on its revived policy of requiring admissions in certain settlements. In FY 2022, the SEC concluded a total of 19 settlements involving an admission of wrongdoing. A common theme running through all these cases was the Commission's finding that the subject company acted in a way that impaired the SEC's investigative function. Seventeen of the cases arose from an industry-wide investigation of broker-dealer recordkeeping practices. The respondents admitted to failing to preserve business-related communications when their employees used personal devices, rather than their employers' systems, in violation of applicable SEC rules. (These cases together also accounted for $1.235 billion out of the $4.194 billion in civil penalties ordered in the year.) The SEC noted that the recordkeeping failures hindered its ability to obtain relevant documents in numerous

investigations. Similarly, in a case against Ernst & Young for a years-long scheme in which certain of its staff cheated on CPA exams, including ethics exams, the SEC secured admissions after finding that the firm improperly withheld relevant evidence during the investigation (though one Commissioner publicly dissented from this finding). Finally, in a case against Allianz Global Investors and three of its former personnel for an extensive scheme of misrepresentations to investment advisory clients, the SEC secured admissions after alleging that the individual defendants attempted to conceal the misconduct from the SEC. While we should not expect the SEC to limit its admission-obtaining policy to circumstances involving obstruction of the SEC's work, such circumstances plainly are aggravating and likely to invite application of the policy. We have seen nothing to change our previously articulated view in last year's memo that this policy does not serve a cognizable public interest goal, but we do not expect any dampening of the SEC's enthusiasm for it.

Whistleblower reports, which reached an all-time high last year at a staggering 76% increase over the previous year, increased yet again in 2022. The number of total whistleblower reports submitted to the SEC hit a new record high of 12,322 tips this year. While the year-over-year increase was small, it showed that the sharp jump in 2021 was not aberrational. The SEC paid a total of $229 million in whistleblower awards in 2022, which was the second highest in any year since the program's inception.

The SEC had a largely successful year in court, at least at the trial level. The Commission prevailed in 12 of the 15 cases it took to trial. In addition, the Commission found success in two noteworthy litigated enforcement actions that we highlighted last year. In *SEC* v. *Panuwat*, the first-ever enforcement action based on the "shadow" theory of insider trading, the Northern District of California denied the defendant's motion to dismiss despite acknowledging that the SEC's theory of liability was "unique." In *SEC* v. *AT&T*, AT&T agreed to settle the case for $6.25 million, the largest penalty ever imposed in a Regulation FD case, following the Southern District of New York's denial of cross motions for summary judgment.

By contrast, the SEC is facing serious setbacks in appellate litigation with respect to one of its two enforcement mechanisms, administrative proceedings before administrative law judges. In *Jarkesy* v. *SEC*, a Fifth Circuit panel concluded that proceedings before administrative law judges are unconstitutional, and vacated the SEC's finding that the respondents had committed securities fraud. In October 2022, the Fifth Circuit denied the SEC's petition for rehearing *en banc*, and the SEC has not petitioned for review by the Supreme Court. A second case in this area, *SEC* v. *Cochran*, is already pending before the Supreme Court, but will likely resolve only the procedural question of whether a respondent can challenge SEC administrative proceedings while awaiting a decision on the merits—a question the *en banc* Fifth Circuit answered in the affirmative. Neither *Jarkesy* nor *Cochran* of course affects the SEC's ability to bring enforcement actions in federal district court.

Some of the Commission's recent rulemaking also has enforcement implications. In October 2022, the SEC approved final rules which require listed companies to implement clawback policies authorizing recovery by a company of incentive-based compensation paid to current or former executive officers during the three prior completed fiscal years if the company restates its financials, regardless of whether there was any misconduct or failure of oversight on

the part of the individual executive officer. In December 2022, the SEC adopted amendments to the Rule 10b5-1 affirmative defense to insider trading liability. The new rule imposes mandatory cooling-off periods, restricts the use of multiple overlapping trading plans, limits the ability to rely on the affirmative defense for single-trade plans, and imposes new disclosure requirements.

The SEC's proposed rules regarding disclosures concerning ESG issues for public companies and investment advisers are still pending. In the event that new rules are ultimately adopted, we can expect heightened enforcement focus in this area. Indeed, the Commission's enforcement staff has not waited for new rules to pursue a variety of investigations in this realm. The cases brought thus far have involved either investment advisers that have not adhered to their disclosures concerning their use of ESG principles in making investment decisions, or companies in environmentally sensitive industries (such as mining) charged with making misleading disclosures regarding significant environmental harms arising from their business operations.

Cybersecurity

In 2021, the Biden administration declared cyber threats a "top priority and essential to national and economic security." This past year has seen that priority translated into concrete regulatory action. In March, the President signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). CIRCIA requires critical infrastructure companies—defined broadly—to report cyber incidents and ransomware payments to the Cybersecurity and Infrastructure Security Agency (CISA). It also requires CISA to promulgate rules implementing the new reporting requirements. In September 2022, CISA issued a Request for Information seeking public input on that project, and we should see some of the fruits of CISA's work in 2023.

Meanwhile, the SEC, which has been active in the cybersecurity realm for over a decade, ramped up its own regulatory efforts with two sets of proposed new cybersecurity-related rules for public companies and for registered investment advisers and funds, respectively. The proposed rules for public companies would require them to disclose cybersecurity incidents more often and with greater specificity; describe their cybersecurity policies, procedures, and governance, including whether and how cybersecurity risks are factored into business strategy and addressed by the board; and report on board members' and management's cybersecurity expertise. The rules for registered investment advisers and funds similarly address cybersecurity incident disclosure and policies and procedures, though they add recordkeeping requirements. Final forms of both sets of proposed rules are expected to issue this spring.

The SEC has also been active on the enforcement side of cybersecurity. Signaling its growing focus on protecting investors from cyber-related threats, the Commission announced in May 2022 that it would double the size of its Crypto Assets and Cyber Unit in the Division of Enforcement. And almost two years after the massive SolarWinds breach, following a lengthy and intensive campaign to gather information from public companies potentially affected by the breach, the SEC served a Wells notice on SolarWinds concerning its cybersecurity disclosures and internal controls and procedures.

Federal authorities are not the only players in this increasingly active field. In November 2022, for example, the New York Department of Financial Services announced proposed amendments to its cybersecurity regulation, originally promulgated in 2017, which would impose heftier cybersecurity-related obligations on financial services companies—including heightened cyber event notification requirements and expanded requirements for risk assessments.

Finally, in the related area of consumer data privacy and protection, 2022 saw the FTC continuing its aggressive enforcement efforts against companies that have failed to adequately safeguard consumer data. In October, the agency took action against online alcohol marketplace Drizly and education technology provider Chegg for their lax security practices that exposed the personal information of millions of their customers. The FTC orders against Drizly—and, notably, also against Drizly's CEO personally—and Chegg, which became final in January 2023, require the companies to limit future data collection and implement a comprehensive information security program.

Cryptoassets

The cryptoasset arena, already a priority enforcement focus for multiple agencies, has confronted even more intense scrutiny since the November implosion of cryptoasset exchange FTX. December saw the sparely-worded but sweeping criminal charges against Sam Bankman-Fried and other former FTX executives—a prosecution of age-old alleged misconduct in a brand new environment. Along with criminal charges, FTX's former executives are facing companion civil enforcement actions by the SEC and CFTC. As this and other, less high-profile matters advance over the coming year, we expect to gain clarity not just about what transpired at FTX in the run-up to its collapse but also about how courts will apply the regulatory framework to cryptoassets and related businesses more generally.

The collapse of FTX was only the latest in a series of recent failures of major centralized cryptoasset-focused institutions, with retail-oriented lending platforms Celsius, BlockFi, and Voyager, and institutional lender Genesis all filing for bankruptcy. Celsius is the subject of investigations or enforcement proceedings by at least 40 states and the federal government relating to its decision to freeze account withdrawals in June 2022, and its founder has been sued for fraud by the New York Attorney General. BlockFi's failure followed its February 2022 settlement with the SEC on charges that it had violated securities laws when it failed to register the offers and sales of its retail crypto-lending product. And Genesis and cryptoasset exchange Gemini now face similar SEC charges of engaging in an unregistered offer and sale of securities to retail investors through a cryptoasset lending program.

The year saw other cryptoasset-focused businesses charged with outright fraud and theft. In February 2022, DOJ arrested the alleged perpetrators of the massive 2016 hack of cryptocurrency exchange Bitfinex, seizing over $3.6 billion worth of bitcoin. In June 2022, the Department announced criminal fraud charges in connection with a crypto-related Ponzi scheme and, separately, what appears to be the largest alleged NFT scheme charged to date. In a burgeoning effort to combat insider trading in the cryptoasset domain, the SEC brought charges against a former Coinbase employee and his associates, and the SDNY charged a former OpenSea employee with fraud and money laundering in connection with frontrunning in NFTs.

Meanwhile, in recent weeks, DOJ, the CFTC, and the SEC all brought actions against an individual who admitted to draining approximately $116 million worth of cryptoassets from a decentralized finance (DeFi) trading platform and publicly defended his actions on the theory that exploiting an identified flaw in open source code is a legitimate trading strategy.

Other enforcement actions in this space have stemmed from the "initial coin offering" wave of 2017-2018. The SEC, for example, recently imposed a springing penalty of up to $30.9 million against Bloom Protocol. A key legal question at the heart of many of these actions is whether sales of the subject cryptoassets constituted illegal securities offerings—an unsettled question first raised prominently in the ongoing *Ripple* litigation, which is now in its third year.

A relatively newer frontier involves nascent enforcement actions implicating decentralized software platforms and decentralized autonomous organizations (DAOs). As to the former, in August 2022, the Treasury Department sanctioned Tornado Cash, a virtual currency mixer that facilitates anonymous transactions, for processing over $7 billion of virtual currency transfers—including for malicious actors. The Tornado Cash sanction came on the heels of Treasury's earlier sanctioning of virtual currency mixer Blender.io, which was used by a North Korea-sponsored cyber hacking group. And concerning DAOs, in September 2022, the CFTC imposed a $250,000 penalty against the organizers of a DeFi protocol and a successor DAO, taking the position that individual members of the DAO could be subject to liability for having participated in token-based governance votes. Enforcement efforts by necessity play catchup to market developments, and in light of regulators' growing scrutiny of DeFi-related abuses, we anticipate more Treasury sanctions and SEC enforcement actions in this area.

One pressing question we expect to be the subject of ongoing discussion through 2023 involves the proper allocation of regulatory authority over cryptoasset-related activities. That question calls out for clarification and is garnering intensified lawmaker attention in the wake of FTX's collapse.

Antitrust Developments

In 2022, DOJ's Antitrust Division and the FTC carried forward their early promises to implement ever more aggressive policies in ever more aggressive ways. DOJ persisted, for example, in applying the antitrust laws to labor markets in novel ways. This untested approach encountered a series of early setbacks with acquittals in *United States* v. *Jindal* and *United States* v. *DaVita*, the first wage-fixing/no-poach cases to reach trial. Recently, however, DOJ was able to secure its first conviction in this area when a healthcare staffing company pled guilty for conspiring with a competitor to allocate employee nurses and fix their wages. And as we summarized earlier this year, the FTC and DOJ also ramped up their challenges to pending mergers—at times animated by novel theories of harm—which have yielded a few wins but also significant pushback from the courts.

Despite some setbacks, there is no sign that either agency will retreat from its aggressive enforcement stance. FTC Chair Lina Khan and Antitrust Division head Jonathan Kanter have both doubled down on their commitment to push the boundaries of antitrust law—particularly in areas where they perceive historical underenforcement. And in November, the

FTC adopted a broad new interpretation of its Section 5 authority to allow it to redress "unfair methods of competition" not reached by the Sherman or Clayton Acts. We saw the exercise of this expanded authority in January 2023, with the agency's first-ever lawsuits challenging contractual noncompete restrictions under Section 5. A day later, the agency proposed a controversial new rule banning noncompete clauses in labor contracts.

Meanwhile, consistent with the broader DOJ agenda, in April 2022 the Antitrust Division updated its flagship leniency program to impose new conditions on immunity. The program—which has remained largely unchanged since 1993—allows organizations that are first in the door and that cooperate fully to avoid criminal prosecution and related fines for antitrust violations. The revised program adds three requirements: the applicant must show that self-reporting was done "promptly"; remedial measures must go beyond restitution and include a root cause analysis; and the applicant must endeavor "to improve its compliance program to mitigate the risk of engaging in future illegal activity."

FCPA Enforcement

FCPA enforcement activity saw an uptick in 2022 from 2021, with DOJ and the SEC resolving a combined total of 12 corporate investigations—four of these by joint DOJ-SEC resolutions with the same companies. On the DOJ side, there were four three-year DPAs (one involving subsidiary guilty pleas), and one plea agreement. Financial penalty figures also rebounded from 2021's level, with DOJ and the SEC imposing a total of approximately $1.6 billion in FCPA-related penalties, disgorgement, and prejudgment interest—about $964 million after credits, including for amounts paid to foreign and other U.S. enforcement authorities. DOJ also issued two declinations under its FCPA Corporate Enforcement Policy. Corporate prosecutions aside, DOJ brought FCPA charges against 13 individuals in 2022—a continuation of a recent downward trend.

The statistics tell only part of the story, particularly because FCPA cases often take a long time to investigate and resolve. But the following insights and trends can be gleaned from the substance of the resolutions:

- ***Wide Variety of Bribery Schemes Captured.*** FCPA resolutions in 2022 involved corrupt payments with objectives that ran the gamut—from obtaining government contracts, to securing favorable tax audit results, to facilitating the passage of legislation, and even to procuring favorable court decisions. U.S. authorities charged with enforcing the FCPA plainly are not limiting their scope or focus.

- ***Independent Compliance Monitors.*** Although it resurrected the independent monitor as an accepted component of criminal resolutions, the Biden administration has thus far been judicious in deploying this tool. Only two of the five DOJ FCPA resolutions in 2022—*Glencore* (resolved by plea agreement) and *Stericycle* (a DPA case)—involved monitors. In each of those, DOJ acknowledged the corporation's remedial efforts but noted that compliance enhancements undertaken in light of the misconduct that gave rise to the charges had not yet been fully implemented and/or tested by the time of the resolution.

- ***Insistence on Strict Compliance with DPA/NPA Obligations.*** In a 2021 policy pronouncement, DOJ signaled it would crack down on less than scrupulous compliance with DPA/NPA obligations. True to that pronouncement, the Department in 2022 extended the terms of two FCPA-related DPA monitorships, in circumstances where a company fell short of its obligations. March 2022 saw the one-year extension of Russian telecommunications company MTS's 2019 DPA, based primarily on the company's need for additional time to fulfill compliance-related undertakings. Then, in December 2022, Swedish telecommunications company Ericsson agreed to its own one-year extension of a 2019 DPA-related monitorship after the company was found to have breached the DPA by failing to disclose relevant information both before and after DPA execution.

- ***Cooperation with International Enforcement Partners.*** Consistent with the Biden administration's December 2021 publication of its U.S. Strategy on Countering Corruption, all but one of the 2022 FCPA resolutions featured some form of international cooperation and/or related foreign enforcement proceedings. Foreign cooperation warranted special mention in connection with Swiss technology company ABB's DOJ-SEC resolution, which involved bribes to a high-ranking government official in South Africa to help secure government contracts. In announcing the DPA with ABB and the guilty pleas of two of its subsidiaries, DOJ touted the matter as the "first coordinated resolution with authorities in South Africa." Separately, discussing the September 2022 resolution with Brazil-based GOL Linhas Airlines involving bribes to secure favorable tax audits, DOJ emphasized its coordination with Brazilian authorities and that U.S. authorities had agreed as part of the resolution to credit payments GOL made to Brazil—a good cross-border example of DOJ's anti-piling-on policy in action.

- ***DOJ Corporate Enforcement Policy.*** The ABB resolution is illustrative for another reason: It evidences DOJ's willingness under its revised CEP to apply leniency even to "recidivists" that fail to self-disclose—provided certain plus factors, like extensive remediation and cooperation, are present. ABB had resolved FCPA-related charges with DOJ and the SEC on two prior occasions, in 2004 and 2010. The compliance program the company implemented in the wake of those run-ins caught the misconduct that formed the basis of the 2022 resolution. The company was planning to self-disclose, but then the media broke the story. In resolving the matter, DOJ required guilty pleas from two subsidiaries, but allowed ABB a DPA without a monitor in view of the strength of its compliance program, its intent to self-disclose, its extensive remediation, and what was described by a senior DOJ official as its "A+ cooperation."

Anti-Money Laundering (AML)

In mid-December 2022, DOJ and the SEC announced a major AML resolution with Denmark-based Danske Bank. The joint resolution required Danske to plead guilty to conspiracy to commit bank fraud and pay total penalties of $2.4 billion (less $1.08 billion in offsets and credits for payments to Danish authorities). As part of the resolution, Danske acknowledged that its Estonian operations lacked adequate AML controls and oversight, and that Danske Bank lied to U.S. banks about its AML controls, transaction monitoring, and high-risk customer base associated with its Estonian unit.

The *Danske* resolution provides another stark reminder of the importance of maintaining a robust AML compliance program, including, as DAG Monaco underscored, "at newly acquired or far-flung subsidiaries."

Other International Enforcement Developments

In October 2022, DOJ brought its first case charging corporate material support for terrorism. French global building materials manufacturer LaFarge and its Syrian subsidiary pled guilty to conspiracy to provide material support to U.S.-designated terrorist organizations the Islamic State of Iraq and al-Sham (ISIS) and al-Nusrah Front (ANF). As part of the resolution, LaFarge agreed to pay a penalty totaling around $778 million and admitted to making payments to ISIS and ANF in 2013 and 2014 to facilitate operation of a cement plant located in Northern Syria. The scheme yielded $70.3 million in revenue for LaFarge, and included a "revenue-sharing agreement" with ISIS that compensated the terrorist organization based on the volume of cement that the company was able to sell its customers.

Notably, LaFarge was acquired in 2015 by a competitor that failed to conduct pre- or post-acquisition due diligence of LaFarge's business operations in Syria. Here again, DOJ took the opportunity to emphasize the importance of investing in robust compliance. In announcing the DOJ's *LaFarge* resolution, DAG Monaco emphasized that this case sends a clear message to all companies, particularly those doing business in "high-risk environments," of the need for appropriately tailored pre-signing and post-closing due diligence in merger and acquisition transactions.

State AG Developments

We expect the high level of state AG activity that we predicted last year to persist across a variety of sectors in 2023 and to expand perhaps into some new areas of enforcement activity. The multi-billion dollar settlements resulting from vigorous prosecutions by state AGs—particularly in the opioid space—are likely to further incentivize state AGs to continue pursuing aggressive regulatory oversight and litigation. Some of the most noteworthy settlements in 2022 included a $26 billion landmark deal with Johnson & Johnson and the three largest U.S. drug distributors, which resolved more than 3,000 opioid-related lawsuits filed by 46 states and other local governments, and the massive opioid settlements with Walmart ($3.1 billion) in November and CVS and Walgreens ($10.7 billion) a month later.

In addition, two notable trends emerged in 2022, which we anticipate will only continue next year:

First, state AGs showed an increased focus on ESG policies, with contrasting stances toward the topic often dividing across partisan lines. For example, we saw Democratic state AGs actively pursue enforcement actions involving so-called "greenwashing" allegations, focusing special scrutiny on the plastics, petrochemical, and chemical manufacturing industries. In April 2022, the California AG launched a first-of-its-kind investigation into fossil fuel and petrochemical companies for their purported role in "perpetuating a myth that recycling can solve the plastics crisis," which so far has resulted in subpoenas against ExxonMobil Corp. and demand letters to six top plastic bag manufacturers. Relatedly, AGs from Massachusetts, North Carolina, and California filed separate lawsuits against numerous chemical manufacturers, alleging that they caused environmental contamination while deceptively advertising their products as safe. At the same time, Republican state AGs seized on novel theories of antitrust and consumer protection laws to launch investigations to challenge ESG initiatives, arguing that coordinated efforts by investor groups and others to pressure companies to reduce their greenhouse gas emissions represent "climate collusion." Most recently, in October 2022, the Missouri AG joined by 18 other state AGs served six major American banks with civil investigative demands seeking information related to the banks' membership in the United Nations' Net-Zero Banking Alliance and other climate-related initiatives. In addition, the West Virginia AG, who in June 2022 won a favorable ruling by the Supreme Court to curb the EPA's efforts to decrease power plants' greenhouse gas emissions, has publicly threatened to sue the SEC for its proposed ESG rules, and most recently led a 21-state coalition to file formal comments against the Commission's proposals.

Second, in the absence of federal legislation regulating data privacy and social media firms, we expect state AGs will continue to fill that vacuum by their increasingly aggressive pursuit of privacy and cybersecurity claims. In March 2022, a bipartisan coalition led by eight state AGs launched an investigation into TikTok, and, in December, the Indiana AG sued the social media company for allegedly deceiving users about China's access to their data and for exposing children to mature content despite marketing the app as appropriate for those 12 years and up. Settlement agreements like Google's $391.5 million settlement with 40 states—the largest ever multistate data privacy settlement—over allegedly unauthorized tracking will likely generate "pile-on" pressure for other states to launch similar actions. Further evidence that states are taking a more aggressive stance against technology companies came in December 2022, when a multistate coalition of AGs across 26 states and the District of Columbia filed an *amicus* brief with the U.S. Supreme Court in the *Gonzalez* v. *Google* case, urging the Court to interpret Section 230 of the Federal Communications Decency Act narrowly to limit the breadth of "publisher" immunity and ensure that technology companies are held accountable under state consumer protection laws for internet-related harms.

Conclusion

Over many years, we have seen both up- and down-cycles in the level and intensity of white-collar criminal and regulatory enforcement activity. We happen at the moment to be in an up-cycle, with more aggressive actions and policy pronouncements. While such up-cycles can sometimes prompt frustration with apparent governmental dogmatism on pet

enforcement issues, these periods also present useful opportunities. Well-managed companies can—and, in our view, should—use the government's heightened attention to compliance effectiveness and tone at the top to searchingly review their current systems and practices, assess whether new policies and/or added resources might be appropriate, and consider the examples presented by enforcement actions taken against other companies, especially those in one's own industry or sector, as offering possible lessons to be learned.

These up-cycles also present, in appropriate cases, opportunities to fight back. For example, when the government is pursuing an untested or questionable legal theory, is misapprehending the key underlying facts, or is failing to consider crucial, mitigating context, a more combative strategy may be called for. In those cases, the combination of thoughtful advance preparation by the subject company to strengthen its overall compliance regime, together with effective, sustained advocacy on the company's behalf, is in our long experience the key to eventual success.

John F. Savarese	David B. Anders
Ralph M. Levene	Sarah K. Eddy
Wayne M. Carlin	Kevin S. Schwartz