January 31, 2022

White-Collar and Regulatory Enforcement:
What Mattered in 2021 and What to Expect in 2022

Introduction

The Biden administration has just completed its first full year in office, and the talk has been tough. New leadership at DOJ, the SEC, the FTC, the CFTC, and other regulatory and law enforcement agencies have issued statements and policy revisions signaling their intention to train more focus on white-collar and regulatory enforcement. We correctly predicted this tougher stance in our wrap-up memorandum last year. What we did not anticipate was the announcement of policies that, depending on how they are implemented, could resurrect what we have viewed as ill-conceived approaches to eligibility for cooperation credit, monitorship imposition, civil penalties, and corporate admissions.

At the Department of Justice, the new leadership includes Attorney General Merrick Garland, Deputy AG Lisa Monaco, and Assistant AG for the Criminal Division Kenneth A. Polite Jr. In her first major speech in October 2021, DAG Monaco announced three significant revisions to corporate enforcement policies that echo initiatives touted by the DAG's Obama-era predecessor, Sally Yates: (1) prosecutors making charging decisions about a company must consider "all misconduct by the corporation discovered during any prior domestic or foreign criminal, civil, or regulatory enforcement actions against it," whether or not the "past misconduct is similar to the instant offense"; (2) any company seeking cooperation credit will once again be required to provide the government with "all nonprivileged information relevant to *all* individuals involved in the misconduct" — not just those whose involvement was substantial; and (3) prosecutors are now encouraged to more often consider imposing monitors as part of corporate criminal resolutions.

At the SEC, Chair Gary Gensler and Director of Enforcement Gurbir Grewal unveiled enforcement policies that track in many respects DOJ's tough stance. These include an unfortunate return to insisting upon admissions of wrongdoing and imposition of independent consultants as prerequisites to settlement in some cases. The SEC also signaled a determination to consider extracting larger civil penalties for white-collar wrongdoers, saying it needs to "make it harder for market participants to simply 'price in' the potential costs of a violation."

We expect it will take some time before the impact of these policies is reflected in the case and penalty data. Below, we discuss the significance of the policy changes and their likely effect on white-collar enforcement over the coming year. We then outline the substantive areas — including accounting fraud, antitrust, cyber security, ESG disclosure, FCPA, and U.S. sanctions — that we expect will attract the greatest attention in 2022. Finally, we review the role we anticipate state Attorneys General will play in the enforcement arena this year.

DOJ Policy Updates

In line with our prediction last year, DOJ leadership appointed as part of the Biden administration has announced its intention to end the four-year period of relatively slower white-collar enforcement under the prior administration. While some of the announced policy changes raise potential concerns, we hope that, as the new DOJ hits its stride, it will provide clarity and transparency concerning the criteria it is applying in exercising prosecutorial discretion, evaluating compliance programs, and granting credit for corporate self-reporting and cooperation.

As noted, the three policy developments DAG Monaco announced in October 2021 seem to auger a return to a tougher, Yates-era program of corporate criminal enforcement.

First, they define corporate "recidivism" broadly — encouraging prosecutors to consider not just prior conduct similar to that currently under investigation but "*all* misconduct by the corporation discovered during any prior domestic or foreign criminal, civil, or regulatory enforcement actions against it," however unrelated it may be to the current conduct. In announcing this approach, DAG Monaco explained that a company's history of misconduct "speaks directly to a company's overall commitment to compliance programs and [whether it has] the appropriate culture to disincentivize criminal activity." This policy could have a particularly significant impact on large financial institutions. By virtue of their size, the breadth of their business, and the intense regulatory scrutiny under which they operate, large banks historically have often found themselves in DOJ's cross-hairs. A policy that holds every error and misstep identified during previous regulatory inquiries against a bank, even in completely unrelated investigations, could lead to unjustifiably harsh outcomes.

Second, by resurrecting the Yates-era requirement that companies furnish information about *all* actors with any involvement in the conduct under investigation, DOJ has sought to limit judgment calls made by company counsel, who can no longer "limit disclosure to those individuals believed to be only substantially involved in the criminal conduct." Explaining the need for this reversal, Criminal Division Chief Polite explained that companies are not always "in the best position to evaluate" who is substantially involved in misconduct and that DOJ may have information that "indicates to [it] which individuals could be helpful to [its] case." Prosecutors are of course entitled to exercise judgment about the scope of their investigation, but we are concerned that this new policy may generate unnecessary delay and resource expenditure and could result in unfairness. Particularly where company counsel has significantly greater familiarity with the facts at the beginning of an investigation and can assist in guiding prosecutors to the important evidence and witnesses, we believe companies should be given full cooperation credit for such efforts and not be second-guessed when they have acted in good faith to substantially assist the government's inquiry.

Third, DOJ's renewed embrace of corporate monitorships may encourage an unwillingness to allow corporations the flexibility to develop and implement their own remedial measures informed by companies' greater knowledge of their own businesses and systems. Our hope is that this new policy will be applied only in those extraordinary cases where the investigation has unveiled a truly broken internal compliance system. And there is some basis for that hope: in explaining the policy, DAG Monaco noted that monitorships will likely be

appropriate only where "compliance program[s] and controls are untested, ineffective, inadequately resourced or not fully implemented at the time of a resolution."

While the full practical impact of these policy changes cannot yet be ascertained, there are signs already that DOJ plans to match its tough talk with more aggressive action. In late December, for example, DOJ resolved investigations involving NatWest Markets PLC and Balfour Beatty Communities LLC by requiring each to enter a guilty plea and accept imposition of a monitor. According to DOJ, these harsh resolutions were warranted because NatWest had breached the terms of a prior NPA and Balfour Beatty Communities had failed to maintain "adequate compliance programs, voluntarily self-disclose misconduct, and fully cooperate with the government."

Having announced these three policy changes, DAG Monaco also announced the creation of a "Corporate Crime Advisory Group" of DOJ personnel tasked with reviewing and proposing changes to corporate criminal enforcement policies and evaluating ways to help prosecutors investigate corporate crime. And she previewed other areas of likely focus over the coming year, including the appropriateness of NPAs and DPAs in cases involving recidivist companies. Depending on just how broadly recidivism ends up being defined, a new policy making it harder to secure an NPA or DPA if a company has an earlier such resolution on its "record" could lead companies to reconsider in the first instance whether to settle or litigate with the government. An NPA or even a no-admit-no-deny settlement with the SEC may appear less attractive as a resolution mechanism if the effect is to seriously limit one's options in future cases. While it is impossible to predict at this early stage, the government's overall enforcement efforts may be impaired and scarce governmental resources stretched if this new policy leads companies to be more reluctant to settle.

Relatedly, DAG Monaco announced an intent, going forward, to "hold accountable any company that breaches the terms of its DPA or NPA." DOJ reportedly has already made good on that commitment, informing Deutsche Bank and Ericsson that they may be in breach of their respective obligations under DPAs entered into during the prior administration for failing to turn over certain factual information. The imperative is thus stronger now than ever to establish robust processes for ensuring compliance with the terms of agreements with DOJ and to strictly monitor those processes. Companies should by no means assume that an NPA or DPA puts past misconduct permanently in the rear-view mirror.

SEC Developments

As with DOJ, the new leadership at the SEC and within the agency's Division of Enforcement have begun their tenure with promises of a more aggressive approach to enforcement. Those promises will not fully bear fruit right away; the investigative process takes time, and further time is required for enforcement recommendations to make their way through the staff's review process and up to the Commission for action. Most of the cases brought in 2021 were the culmination of investigations commenced under the prior administration. But the current administration's announced approach is discernible in recent charging decisions and settlement terms.

The Commission brought a total of 434 standalone enforcement actions in its fiscal year ended September 30, 2021. This was a 7% increase over the more significantly pandemic-disrupted fiscal 2020, though it was still somewhat below pre-2020 levels. The case mix was in line with historical patterns. Public company disclosure and accounting cases were about 12% of the total. (Securities offerings comprised 32% of the cases, but many of these involved unregistered offerings, Ponzi schemes, etc. — rather than offerings by public companies.) Insider trading cases always get a degree of attention out of proportion to their share of the enforcement pie — in 2021, they were 6.5% of the cases brought, within the historical range.

The whistleblower program continues to be an important component of the SEC's enforcement effort. In fiscal 2021, the SEC received a total of 12,200 whistleblower reports, a staggering 76% increase over 2020, which was the previous annual high water mark. The largest categories of reports in 2021 were manipulation (25%), corporate disclosure and financial reporting (16%) and offering frauds (16%). The concrete results traceable to whistleblower information also reached new heights in 2021. The Commission awarded more whistleblower payments in 2021 — a total of $564 million — than in all prior years combined, dating from the inception of the program in 2011. The whistleblower program also continues to illustrate the importance of thoughtful efforts by companies to address compliance concerns when they are raised by corporate personnel. Approximately 60% of the 2021 award recipients were current or former insiders of the entity about which they reported information to the SEC. Of those awardees, 75% say they raised their concerns internally before making a report to the SEC. At least some portion of these represent lost opportunities to address a problem before it got worse.

"Aggressiveness" in SEC enforcement can take many forms. A more zealous approach may, for example, lead the Commission to authorize charges where critical factual elements are in dispute. A recent example is an insider trading case involving the "shadow theory," in which an employee of a biopharmaceutical company who received information about the potential acquisition of his employer then traded in the securities of another company in the same small industry segment. Another recent illustration is a case brought under Regulation FD involving alleged selective disclosure of material nonpublic information to sell-side analysts. Both cases are in litigation. The SEC has a long history of bringing reasonable cases that further its enforcement program goals even where victory at trial is not assured. But a conscious effort to be seen as more aggressive can sometimes go hand-in-hand with questionable charging decisions. We saw this in the wake of the financial crisis, for example, when defense advocacy and/or contested litigation revealed that a number of cases the SEC brought against individuals lacked sufficient supporting evidence.

A desire to present a more aggressive profile can also translate into changes in enforcement policy. The new SEC leadership has, for example, spoken of a desire to increase the level of civil money penalties imposed in settlements. The penalty amount pendulum has swung back and forth with the change of administrations for decades. What is often overlooked is that the SEC's authority to obtain penalties is statutory and subject to specific dollar limitations. This has sometimes not prevented the SEC from seeking or obtaining through settlements penalty amounts that would be virtually impossible to obtain in litigation before a judge bound to apply the statutory criteria. It is our hope that the SEC will stay mindful of the

limitations on its penalty authority, and not seek settlement terms that would be unobtainable even in the event of complete success in contested litigation.

The new aggressiveness at the SEC has also been reflected in a revival of the policy of seeking admissions in certain settlements. This is a regrettable development that serves no articulable public interest. In the wake of the Commission's decision under then-SEC Chair Jay Clayton to edge away from his predecessor's innovation of requiring admissions, we have seen no development in the securities markets, no upswing in any category of violations, no diminution in the perceived significance of SEC settlements, nor any other reason to suggest discontinuance of the admissions experiment was anything but well-advised. The SEC already has ample methods to exhibit "toughness" in framing enforcement actions without the need to exact admissions. These include administrative orders and injunctive complaints that describe violative conduct in detail, civil penalties in appropriate measure, thorough remedial undertakings where warranted, and public commentary by members of the Commission and senior enforcement staff. The Commission's long-standing policy of settling cases on a no-admit-no-deny basis was not an effort to go easy on wrongdoers. Rather, it was intended to encourage and facilitate settlements by limiting collateral effects in proceedings not involving the SEC. The policy made settlements more feasible, and avoided unwarranted expenditure of resources in cases that could otherwise be resolved. The policy produced tangible gains in the public interest.

Finally, the SEC is pursuing a variety of policy goals that may signal future enforcement attention. For example, the Commission has published for comment proposed changes in the rules governing share repurchases by issuers and the use of 10b5-1 plans by corporate officers and directors. The interest in pursuing policy changes may heighten the likelihood of an enforcement inquiry in the event that information comes to the staff's attention suggesting possible violations in these areas. Neither area, however, has historically been a focus of enforcement activity and the pending rulemaking process is the proper method for considering changes in regulation.

Update on Main Areas of Substantive Focus

A. Uptick in accounting fraud investigations

In recent years, we and other observers noted some diminution in the number of major SEC accounting fraud and disclosure investigations. But 2021 saw an uptick in enforcement activity in this area, and we expect that trend to continue. At a high level, audit and accounting charges, including cases where issuers' financial disclosures were found misleading, represented 12% of all SEC actions in FY 2021. At least one of those cases originated from the Enforcement Division's EPS Initiative, which uses data analytics to seek out potential instances of accounting and disclosure violations caused by, among other things, earnings management practices. The no-admit-no-deny settlement with Healthcare Services Group, Inc. and its CFO and controller involved a failure to timely accrue for and disclose material loss contingencies. In settling negligence-based antifraud violations on August 24, 2021, the company agreed to pay a $6 million penalty.

Among the other accounting cases brought by the Commission in the latter half of 2021 was the settled enforcement action against Kraft Heinz Co. and two former senior executives arising out of a long-running expense management scheme. According to the SEC's order, Kraft improperly recognized unearned discounts from suppliers and maintained false supplier contracts — then publicly touted the resulting "cost savings." The settlement terms included negligence-based antifraud violations of Section 17(a), internal accounting controls and books-and-records violations, and a $62 million civil penalty. More recently, on December 6, 2021, the SEC charged American Renal Holdings, Inc., a national provider of dialysis services, and three of its executives with securities fraud and other misconduct. According to the SEC's complaint, filed in the Southern District of New York, the company engaged in a so-called "cookie jar" scheme which involved using opportunistic revenue adjustments to create the false impression that the company had beat, met, or come close to meeting its numbers.

B. Antitrust Enforcement

As we predicted last year, antitrust enforcement began ramping up in 2021 and will likely continue apace in the coming years. With the Senate's confirmation of Lina Kahn as FTC Chair in June 2021 and of Jonathan Kanter as AAG for the DOJ's Antitrust Division in November 2021, companies can expect to see aggressive antitrust enforcement, on both the civil and the criminal sides, aimed not simply at conduct that increases prices or reduces competition, conventionally defined, but also at enterprises that the new administration deems so large and powerful as to be market-distorting. In a recent speech, AAG Kanter underscored the message that his Division will use more aggressive tactics in seeking to preserve competition and be willing through litigation to revisit settled antitrust law precedents.

Some of the actions launched last year, including the lawsuit filed by the FTC against Facebook alleging that the company engaged in an illegal "buy-or-bury scheme" to maintain its dominance, and the Antitrust Division's suit to block Penguin Random House's acquisition of rival publisher Simon & Schuster, are emblematic of this new thinking, as are several high-profile ongoing investigations of large tech companies. We do not see this trend abating any time soon, unless litigation challenges lead to court rulings finding that these newly deployed theories are not legally or factually tenable. The litigation results to date have been mixed. Just two weeks ago, the trial court in the Facebook case, while substantially narrowing the scope of the FTC's theory, ultimately denied the company's motion to dismiss in part.

C. Cybersecurity

The Biden administration has declared cyber threats a "top priority and essential to national and economic security." In 2021, the White House even published an unprecedented open letter urging corporate leaders to treat the risk of cyberattack as a threat not just to data security but to core business operations generally. The threat becomes more acute every year, but the Covid-19 pandemic, with its mass shift to remote work arrangements and increased reliance on cloud-based operations and virtual commerce, has accelerated our collective vulnerability. Among the notable attacks of 2021 were the massive SolarWinds breach and the ransomware attack that shut down one of the country's largest pipelines for refined petroleum products.

The enforcement response to cyber threats increasingly has extended beyond pursuit of the prime malefactors — the cybercriminals and their backers who initiate and coordinate the attacks — to focus on the detection of, response to, and disclosure of cyberattacks. In other words, the lens increasingly has become trained on companies that can expect to find themselves targets of cybercrime. We saw this, for example, with the SEC enforcement action against First American Financial Corp., the no-admit-no-deny settlement of which was announced in June 2021. According to the SEC, technical experts at FAFC, a real estate settlement services provider, discovered a vulnerability in the company's systems but failed to report it up the chain, disclose it, or remediate it. The vulnerability was addressed only months later, after a journalist highlighted it, and the company's public response failed to disclose that the problem had been discovered earlier. The SEC charged FAFC with failure to maintain disclosure controls and procedures, in violation of Rule 13a-15(a).

A similar enforcement action was announced in August, this time against Pearson plc, which provides academic performance assessment services. According to the SEC, Pearson made misleading, boilerplate public disclosures about cyber risks that failed to acknowledge — much less highlight — a breach that had resulted in the unauthorized extraction from its systems of substantial personal data concerning students and school administrators. When the media discovered the breach, Pearson responded with what the SEC called materially misleading statements designed to downplay the scale and seriousness of the intrusion.

The SEC is not the only agency focused on shoring up cyber defenses through enforcement actions directed at corporate cyber compliance programs and disclosures. In October, DAG Monaco announced a new Civil Cyber-Fraud Initiative targeted at companies who "fail to follow required cybersecurity standards," thereby "put[ting] all of us at risk." The Initiative, which will be led by the Civil Division's Commercial Litigation Branch, Fraud Section, is tasked with using the False Claims Act — and its attendant whistleblower provisions — to identify and pursue actors who knowingly "provid[e] deficient cybersecurity products or services," misrepresent their cybersecurity practices and procedures, or fail to monitor or report breaches.

We expect that 2022 will bring more in this vein, and that companies will come under even greater pressure not only to ensure that their cybersecurity systems and disclosures withstand close scrutiny but also to cooperate with government efforts to identify and redress cyberattacks. A company's best defense against these looming regulatory and litigation risks is to run regular cyber preparedness drills, periodically test and enhance the efficacy of cybersecurity systems, and put effective procedures in place to ensure that information about breaches and risks is surfaced to the right levels within the organization so that decisions about disclosure obligations, if any, are made with complete and up-to-date information.

Another development we expect in 2022 is increased cooperation among agencies focused on cybersecurity, on the one hand, and cryptocurrency, on the other — especially since the latter is so often used to facilitate cyber breaches. Indeed, the same day the DAG announced the Civil Cyber-Fraud Initiative, she also announced the creation of a new National Cryptocurrency Enforcement Team. The idea behind the NCET is to combine DOJ's expertise in combatting money laundering and cybercrime under one umbrella and "tackle complex investigations and prosecutions of criminal misuses of cryptocurrency, particularly crimes

committed by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors."

D. ESG Disclosure

Many commentators over the past year have noted the increased focus on corporate ESG disclosures, and we expect this trend will be accompanied by an increase in SEC enforcement and other litigation risks for companies whose disclosures in this area are found to be inaccurate or misleadingly incomplete. One important signal of this increased attention came on March 4, 2021, when the SEC announced the creation of a Climate and ESG Task Force within its Division of Enforcement. The Task Force's stated ambition is to identify misstatements in companies' disclosures of climate risks, find gaps in existing disclosure requirements, and analyze disclosure and compliance issues relating to investment advisers' and funds' ESG strategies. The SEC's Acting Corporation Finance Director has elaborated that new disclosure requirements will focus on three areas: diversity, equity, and inclusion; climate change; and human capital management. And, in August 2021, SEC Chair Gensler announced that the Commission is actively considering near-term rulemaking that would mandate climate change-related disclosures, including as to oversight and management of climate-related risks and opportunities. Although no new rules have yet been promulgated, the SEC released a sample letter in September with requests it may make of companies to ensure they comply with prior SEC guidance on climate change disclosures. This year we are also seeing Corporation Finance letter inquiries to numerous companies seeking clarification and/or amendment of climate change disclosures.

In an important speech in November 2021, Commissioner Crenshaw noted that, "with ESG now front and center, the reliability of corporate ESG risk disclosures, and their potential impact on and connectivity to financial statements, is critical." Crenshaw's conception of ESG is very broad, encompassing cybersecurity and climate risk. As she put it, "I do not think I am alone in wanting to understand how companies are determining whether and how financial statements are impacted by climate change risk; how assumptions used to reach these determinations are set, tested, and reevaluated over time; and how any existing disclosures are being formulated." With this spotlight on ESG disclosures, companies must take particular care to adequately vet their accuracy and reliability. As companies strive to expand their disclosures in this area, the risk of misleading statements may increase, along with an increased number of shareholder suits and government enforcement proceedings.

E. FCPA

By the usual statistical measures, 2021 was a significantly down year for FCPA enforcement. In brief, DOJ and the SEC together resolved three corporate investigations involving FCPA charges, two of which were joint resolutions involving the same companies. The third was an SEC-only resolution. The DOJ resolutions were by DPA and the SEC cases by settled administrative proceedings. DOJ and the SEC also resolved related criminal and civil investigations into Credit Suisse AG's financing of projects in Mozambique that involved substantial corrupt payments to foreign officials and other misconduct, but the cases were charged under the criminal wire fraud statute on the DOJ side and the anti-fraud and internal accounting control and books and records provisions of the federal securities laws on the SEC

side. The enforcement theory was that Credit Suisse defrauded investors in the financing instruments it helped to issue to fund the projects, including by failing to make proper disclosures about the risks of corruption in the underlying projects.

Total financial penalties in 2021 for corporate FCPA resolutions were also significantly down from recent years, with DOJ and the SEC imposing a total of some $183 million in penalties, disgorgement, and prejudgment interest. After offsets paid to foreign enforcement authorities in resolution of parallel investigations, recovery totaled about $160 million. (The Credit Suisse case involved an additional total of approximately $275 million in fines, penalties, and interest paid to DOJ and the SEC after giving credit for payments to foreign and other U.S. enforcement authorities.)

No declinations were issued in 2021 pursuant to DOJ's FCPA Corporate Enforcement Policy, and, on the individual side, DOJ brought criminal cases against 18 defendants — on the low end of the historical range for such cases.

The real action in 2021, however, was what the new administration said and did to lay the groundwork for what we expect will be vigorous FCPA enforcement in the coming years. In March, media reports noted that the number of prosecutors in DOJ's FCPA unit had hit a record level, and that the unit had also hired an attorney with substantial private sector compliance expertise, including service on the monitor team for DOJ's 2016 FCPA resolution with Brazilian petrochemicals firm Braskem, one of the largest resolutions in history. In June, President Biden issued a National Security Study Memorandum which declared the fight against corruption abroad a "core national security interest." The NSSM set in motion an intergovernmental review process aimed at developing a comprehensive and coordinated strategy across governmental departments and agencies to significantly enhance the government's ability to address foreign corruption and hold those responsible for it accountable.

In speeches, announcements, and other actions in 2021, U.S. authorities underscored the President's message that fighting foreign corruption would be a major priority. These included the issuance of Treasury Department sanctions against three foreign individuals and 64 related companies for involvement in corruption in Bulgaria, the creation of a joint task force to coordinate and enhance enforcement efforts against corruption and human and narcotics trafficking in Mexico and the Northern Triangle of Central America, and a signal to corporate America from a senior DOJ official speaking at a prominent anti-corruption conference that the DOJ intended to be more active in developing its own FCPA case leads, as opposed to simply relying on corporate self-reporting.

In early December, the Biden administration issued the U.S. Strategy on Countering Corruption presaged by the NSSM. The Anti-Corruption Strategy, which is described as a "whole-of-government approach to elevating the fight against corruption," rests on the following "five distinct, mutually-reinforcing strategic pillars": (i) modernizing, coordinating, and resourcing U.S. government efforts to fight corruption; (ii) curbing illicit finance; (iii) holding corrupt actors responsible; (iv) preserving and strengthening the multi-lateral anti-corruption architecture; and (v) improving diplomatic engagement and leveraging foreign assistance resources to advance policy objectives. The "pillars" are supplemented by

enumerated action items, which are detailed in an extensive appendix. We highlight two key takeaways for corporations:

First, consistent with the U.S. government's decades-long efforts to promote anti-corruption enforcement by foreign governments, the Anti-Corruption Strategy emphasizes efforts to enhance existing international institutions and frameworks (such as the OECD), and the development of new mechanisms for international cooperation — including more extensive information sharing — with both governmental and non-governmental parties, including investigative journalists who seek to identify and expose international corruption.

Second, the Anti-Corruption Strategy highlights efforts to protect the U.S. financial system and U.S. investment from exploitation by illicit actors, who launder or shelter the proceeds of corruption, by deploying new tools, such as the creation of the beneficial ownership registry of certain domestic and foreign companies registered to do business in the U.S. as provided by the Corporate Transparency Act ("CTA") and use of the pilot whistleblower program under the Kleptocracy Asset Recover Awards Act, both of which were enacted in January 2021. In December 2021, FinCEN issued the first of three proposed rulemakings — focused on the beneficial ownership reporting standards and requirements — to implement the CTA's requirements. The Anti-Corruption Strategy also calls for (i) new Treasury regulations adding reporting requirements on real estate transactions; (ii) re-visiting minimum AML and suspicious activity reporting standards — first proposed in 2015 — for investment advisors overseeing investment vehicles such as hedge and private equity funds; (iii) consideration of additional tools, including by legislation if needed, to address service providers such as trust companies, incorporators, corporate service providers, lawyers, accountants, and registered agents/corporate nominees involved in facilitating sheltering and investment of illicit proceeds; and (iv) assessment of additional enhancements to the current federal AML regime. As these efforts are likely to have significant effects on banks, investment firms, and others in the financial, wealth management, and related sectors, it will be important to monitor developments and ensure that on-boarding and AML monitoring programs are kept up-to-date.

While it remains to be seen just how fast and effectively the government is able to implement its new Anti-Corruption Strategy, much of which may depend on appropriate funding, we believe corporate boards of directors and senior management should take the administration at its word regarding a coming era of more aggressive anti-corruption enforcement. This aggressive rhetoric concerning anti-corruption efforts is, of course, consistent with the administration's broader messaging described above reflecting a more determined approach to white-collar and regulatory enforcement by DOJ, the SEC, and other U.S. enforcement authorities. It is worth remembering in this regard that the FCPA Corporate Enforcement Policy has *not* been changed, and thus continues to provide an opportunity for companies to secure either prosecution declinations when they promptly self-report or significant fine reductions when they provide complete cooperation even in an investigation initiated by DOJ.

F. Sanctions

In October 2021, Department of the Treasury issued the results of a broad-based review of the economic and financial sanctions programs it administers that had been initiated by the Biden administration. In affirming the importance of sanctions as a powerful tool to address

national security and other government interests, the review called for action along the following lines to ensure continued effectiveness of sanctions in light of developments, such as digital assets, new payment systems, and the rise of strategic economic competitors, that have given rise to new ways of hiding cross-border transactions and evading the reach of current sanctions: ensuring that (i) sanctions are used to pursue specific objectives within a larger strategic framework; (ii) where possible, efforts are made to maximize sanctions effectiveness through multilateral coordination with allies and engagement with other stakeholders, including financial institutions and other companies; (iii) sanctions are calibrated to mitigate unintended economic, political and humanitarian consequences; (iv) sanctions are easily understood, enforceable and, where possible, can be reversed as appropriate; and (v) the Treasury's sanctions-related technology, workforce, and infrastructure are modernized.

As reflected in the Treasury's review, the use of sanctions has steadily increased over the last 20 years, and this trend can be expected to continue as sanctions are imposed in service of national security and other policy and enforcement goals. Indeed, the Anti-Corruption Strategy cites the use of economic sanctions, especially in coordination with partner governments, as a key tool to curtail foreign corruption. As a result, it is important for financial institutions and companies doing business internationally to stay abreast of sanctions (and related export control) developments and ensure that such developments are reflected in their compliance programs as appropriate.

Role of State AGs

In last year's memorandum, we predicted that state AGs would remain active in their regulatory oversight, having become increasingly empowered during the past administration. That has proved true, as state AGs continue to vigorously pursue enforcement actions across a variety of sectors including consumer protection — with notable focus on opioids and vaping — and antitrust. In a sign that this trend will persist, a bipartisan coalition of 32 state AGs sent a letter to Congress in September 2021 proclaiming their support for six bills that would strengthen the ability of state AGs to pursue antitrust actions. As we have noted, investigations by state AGs are notoriously challenging to navigate as each state AG may have his or her unique enforcement priorities and, given the political nature of the state AG position, considerations other than simply the merits can affect how investigations are resolved.

Conclusion

Both DOJ and the SEC are emphasizing self-reporting and cooperation. As Director of Enforcement Grewal noted in a recent speech, boards of directors and management "also have a key role to play in spotting and addressing emerging risks, and that's both by ensuring that your proactive compliance efforts continue even after violative conduct has occurred and by working with us in addressing that conduct. Firms' cooperation with our investigations, including through voluntary self-reporting of potential violations, benefits all market participants."

In keeping with that admonition, and with the stage set in 2022 for greater regulatory and criminal enforcement over the remainder of the Biden administration, we offer the same advice as we have in the past, with perhaps even greater emphasis: well-managed

companies and attentive boards of directors would be wise to continue investing in the design, implementation, and periodic evaluation of a robust compliance program tailored to the company's business activities and regulatory and legal risks, as those evolve over time. Effective compliance programs provide the surest foundation for preventing misconduct from arising in the first place or nipping potential legal and compliance issues in the bud before they blossom into a full-blown corporate crisis. And should misconduct occur, an effective compliance program that enables early detection and timely remediation will best position a company to achieve the most favorable resolution at the close of any resulting investigation. Good compliance, as we've often said, is fundamental to securing business success and stability.

John F. Savarese	David B. Anders
Ralph M. Levene	Sarah K. Eddy
Wayne M. Carlin	Carol Miller