January 18, 2017

White Collar and Regulatory Enforcement: What to Expect in 2017

Introduction

As in so many areas of public policy, it is very difficult, if not impossible, at the moment to provide any reliable prediction of how the new Administration may change white collar and regulatory enforcement priorities, policies or practices. What is certain is that things will change. But where and how will those changes come?

Neither Attorney General-designate Jeff Sessions nor President-elect Donald Trump has offered any significant insight into their thinking in this important area, (although Sessions did suggest at his confirmation hearings that perhaps corporate officers who engaged in wrongdoing should be subjected to more severe punishment than the company itself).

Nor have congressional leaders signaled any particular changes that they expect to see implemented or that they will push to enact. Thus, in the absence of any clear guideposts, we thought it would be unwise to offer predictions. But we did think it might be helpful and appropriate to suggest some areas where measured, considered change would be beneficial. Our suggestions follow:

- We think it would be sensible and appropriate for the Department of Justice and other prosecutors to exercise greater restraint and caution when considering whether to impose monitorships on companies that resolve white-collar or regulatory inquiries. As some commentators have observed, such monitorships can be highly intrusive upon company operations and management, are often extraordinarily expensive, stretch on for years, and, most importantly, can be unfocused in their scope and, in many instances, are unsupervised by courts;

- DOJ, as well as other prosecuting bodies, should give greater weight to a company's pre-existing compliance program when

considering whether to initiate a prosecution or to seek a criminal disposition of an inquiry. This is already a factor that is required to be considered by both the DOJ's Principles for Federal Prosecution of Business Organizations (USAM 9-28.800) and the U.S. Sentencing Guidelines for Organizations (Section 8B2.1). But, in our experience and that of other experts in this field, a company's good faith effort to implement a well-designed set of compliance policies and procedures is often, in practice, inadequately rewarded when prosecutors consider the use of criminal law to resolve problems that may arise, notwithstanding the careful adoption and implementation of such compliance programs. We believe that if DOJ and other prosecutors were to give more concrete and substantial credit to companies that have implemented well-designed compliance programs, this would have the salutary effects of reducing misconduct *and* incentivizing all companies to devote more resources to building and maintaining effective compliance programs. Congress, for its part, should consider, as an initial step, amending the Foreign Corrupt Practices Act to include a specific affirmative defense for having had in place an effective compliance program, which could be patterned after Section 7 of the U.K. Bribery Act of 2010;

- DOJ should embrace more demanding and thoughtful methods to review the exercise of prosecutorial discretion in order to avoid the sort of misguided prosecutions that are illustrated by the much-criticized and unsuccessful prosecution of Federal Express in the Northern District of California. Corporate prosecutions should be predicated on solid evidence of a truly deliberate effort to violate or evade known legal requirements engaged in by responsible actors within a corporation; companies should not be prosecuted simply for inadvertent failures to prevent harm. The Federal Express prosecution is a telling example of how the failure to focus on those factors can lead to wasteful and failed prosecutions and impose enormous costs on enterprises that engage in no criminal wrongdoing. DOJ's almost complete failure to convict the former BP employees who were prosecuted in the wake of BP's

Deepwater Horizon drilling platform explosion and resultant oil spill, similarly shows that criminal prosecutions are not necessarily the right response to events that cause tragic, costly and significant harm. The alternative of relying upon civil and regulatory remedies -- consideration of which is already called for by the USAM -- should receive greater attention and be given greater weight when prosecutors evaluate the appropriate mechanism for resolving a criminal inquiry;

- Likewise, it would be a salutary development for DOJ prosecutors and other regulatory enforcement agencies to be reminded that they should not use the instrument of criminal law enforcement to effect back-door changes to established regulatory regimes. Such changes should only be made pursuant to the requirements of the Administrative Procedure Act or through congressional action (Arlen, "Prosecuting Beyond the Rule of Law: Corporate Mandates Imposed Through Deferred Prosecution Agreements"); and

- Congress and DOJ should consider the inclusion of the element of scienter in all white collar criminal statutes, or, at a minimum, conduct a comprehensive reappraisal of federal criminal laws to assess the need for an express scienter element where appropriate, as has been proposed in connection with the Federal Sentencing Reform Act, currently pending in Congress.

Whatever the future may hold, however, it is clear from developments over the past year that companies will continue to face substantial and familiar risks in the white collar and regulatory arena. In the sections that follow, we provide our views on what companies can fairly expect to see in 2017 concerning:

- The Yates Memorandum (p. 13); and
- SEC developments (p. 14).

Developments in Cybersecurity

Corporations continue to be buffeted by a storm front of cyber-related risks, primarily the product of relentless efforts by cyber criminals to breach networks; obtain personally identifiable information (PII) and other valuable data; encrypt or destroy corporate systems; and steal intellectual property. No longer localized in any particular geographic area or economic sector, the cyber storm now affects companies in all lines of business and all parts of the world. Breaches at organizations that range from the high-tech industry to the political arena, and include entities as technologically sophisticated as LinkedIn and as large as the United States government, have demonstrated that no system is immune from attack. As cyber risks increase in intensity, corporate leaders must continue to invest time and resources in achieving sound cybersecurity through thoughtful security assessment, deployment of cutting-edge technology, employment of experienced security leaders, engagement in incident response planning, and adoption of sound risk mitigation strategies.

But companies and executives also face a second front of risks posed by regulators and civil litigants. Companies must navigate a complex regulatory environment, as more and more agencies at the state, federal and international levels enter the cybersecurity landscape. An expanding web of cyber-incident disclosure laws, regulatory requirements, and best-practices expectations poses daunting compliance challenges. And cyber incidents are followed with increasing frequency by waves of civil lawsuits brought by customers, investors, and affected third parties.

Regulators have begun to shift enforcement focus from companies that have failed to take basic precautions to those that have made significant, albeit unsuccessful, investments in cybersecurity. In a June 2016 enforcement action, the Securities & Exchange Commission (SEC) held a financial industry leader accountable for the actions of a rogue employee who circumvented internal controls and database restrictions to transfer customer data to his personal server, which in turn was hacked by a third party. While the company's self-detection and reporting of the insider breach earned the company treatment as a victim and a large restitution award from federal law enforcement, the SEC nevertheless found

that the company's controls suffered from technical, monitoring and auditing deficiencies, ultimately resulting in a settlement carrying a $1 million penalty. This action highlights the sometimes schizophrenic government response to instances in which companies experience cyber incidents. It also serves as a reminder that companies should invest not only in state-of-the-art data protection, but also robust monitoring and auditing systems.

At the same time, some agencies are taking a new, more prescriptive approach to cyber regulation. In October 2016, the New York State Department of Financial Services (NYDFS) unveiled proposed regulations requiring covered institutions – entities authorized under New York financial services laws – to meet strict minimum cybersecurity standards, including mandatory procedures, onerous notification requirements, and board-level compliance certifications. Intense industry pushback resulted in NYDFS easing the regulations somewhat, but they remain hands-on and potentially onerous. Meanwhile, federal banking regulators, in commencing a public comment process on upcoming cyber regulations, asked for input regarding whether they should follow suit by mandating granular cybersecurity requirements and imposing oversight obligations on boards of directors. Corporations across all industries should monitor these developments closely, as the new rules are likely to serve as models for regulators outside the financial sector.

In order to limit potential liability, corporate leaders need to engage in robust cybersecurity preparation at all levels of the company, from the board of directors to the entry level. At the board and executive level, companies should institute an effective system of cyber governance; at the information security level, companies should invest strategically in technology, testing and talent; and throughout the business, companies should prioritize training to assure top-notch cyber hygiene. Doing so will not only mitigate cyber risk, but help protect corporations and their leadership teams from liability.

Cross-Border Enforcement Developments

A. Panama Papers

In April 2016, media reports announced a massive leak of some 11.5 million documents from the electronic files of Panama-based law firm Mossack Fonseca, which is reported to be one of the top providers of offshore corporation and trust services through offices located in dozens of jurisdictions around the

world, including Liechtenstein, the British Virgin Islands, Dubai, Switzerland and the U.S. The files, which have come to be called the "Panama Papers," detail information on more than 200,000 offshore companies and trusts established and/or managed by the Mossack Fonseca firm, and were eventually posted on the Internet by the International Consortium of Investigative Journalists, an organization which has been active in publishing data and reports on offshore tax evasion and other activities based on other leaked information. The Panama Papers set off a flurry of media reports focused on connections between Mossack Fonseca offshore structures and high-profile individuals and political figures, such as close associates of Russian President Vladimir Putin, Chinese Communist party officials, former British prime Minister David Cameron's father, and Iceland's then Prime Minister, who resigned in the face of reports of his interest in an offshore structure set up by Mossack Fonseca.

Governmental authorities and regulators around the world have initiated inquiries as a result of the Panama Papers leak, along with a variety of regulatory proposals aimed at increasing transparency in offshore structures and making it more difficult to use such structures to support money laundering and other illegal activities. In the U.S., the U.S. Attorney's Office for the Southern District of New York ("USAO") and DOJ are reported to be conducting a criminal investigation concerning matters related to the Panama Papers, and NYDFS is reported to have requested that more than 15 banks, including numerous foreign banks with offices in New York, provide information on the Mossack Fonseca firm. To date, NYDFS has brought the only enforcement action directly citing the Panama Papers or Mossack Fonseca against the New York branch of Taiwan-based Mega Bank, which included focus on business activities between the bank and its Panamanian affiliates. In addition to findings of serious deficiencies in the New York branch's BSA/AML compliance programs and controls, NYDFS reported that its probe had determined that a "substantial number of customer entities, which have or had accounts at several branches, were apparently formed with the assistance of the Mossack Fonseca law firm in Panama. (NYDFS Press Release, dated August 19, 2016) Mega Bank entered into a Consent Order that included payment of a $180 million penalty and imposition of an independent monitor, among other undertakings related to the implementation of an effective AML compliance program.

While there has been significant press and regulatory attention, it remains to be seen whether the Panama Papers leak will result in significant

enforcement activity. In the interim, the matter serves as an added reminder of the importance for financial institutions to maintain effective Know Your Customer/Due Diligence, AML surveillance and AML investigation programs.

B. **Cross-Border Tax Enforcement**

Furthering a trend going on ten years now, 2016 saw the DOJ and IRS continue to press their enforcement efforts in the area of cross-border tax. A significant milestone in this area was the announcement in the waning days of 2016 that the DOJ had reached the final resolutions in its Program for Swiss Banks. That Program, first announced in August 2013, provided a means for Swiss banks not already under U.S. criminal investigation (the so-called "Category 1 banks") (i) to resolve through a non-prosecution agreement ("NPA") potential U.S. criminal liability for past conduct involving undeclared U.S. accountholders, or (ii) to obtain a non-target letter ("NTL") to the extent that the Swiss bank could demonstrate that it had not engaged in past misconduct involving U.S. accountholders. All totaled, DOJ entered into 78 NPAs covering 80 Swiss banks and another similar NPA with a Swiss asset manager, with total penalties of approximately $1.3 billion. DOJ also entered into NTL's with 5 Swiss banks.

While DOJ and IRS acknowledged that the Program would enter a "legacy" phase, senior officials underscored that the enforcement effort would continue. Principal Deputy Assistant AG Caroline Ciraolo said that DOJ "will continue to hold financial institutions, professionals and individual U.S. taxpayers accountable for their respective roles in concealing foreign accounts and assets and evading U.S. tax obligations." Indeed, beyond the significant dollars obtained in penalties and the compliance changes leading to greater transparency required to be implemented by banks participating in the Program, banks that entered NPAs were required to provide information about former client accounts, including banks in Switzerland and other countries to which accounts or assets were transferred, and to cooperate with ongoing U.S. investigations relating to their past conduct and U.S. related accounts. Additional enforcement activity is to be expected as DOJ and the IRS use such information to develop leads on new cases involving accountholders, financial institutions and third-party facilitators assisting undeclared U.S. taxpayers both in Switzerland and elsewhere. With the Program concluded, we also expect DOJ to resolve the remaining Category 1 Swiss bank investigations.

Outside of the Program, there were two significant bank resolutions in 2016. In February, DOJ announced that Bank Julius Baer, a Category 1 Swiss bank, had entered into a three-year deferred prosecution agreement ("DPA") with the USAO to resolve DOJ's long-running investigation of the bank's involvement with undeclared U.S. taxpayers. The resolution included the filing of a one-count criminal information charging the bank with conspiring with undeclared U.S. taxpayer clients to defraud the IRS, and an acknowledgement that the bank had knowingly assisted many of its U.S. accountholders in evading their U.S. tax obligations. Julius Baer agreed to pay $547 million in disgorgement, restitution and a criminal fine and to cooperate with DOJ's continuing investigative efforts. Related to the resolution, and with Julius Baer's encouragement, two client advisors originally charged in 2011 who had remained abroad, came to the U.S. and pled guilty to charges of conspiring with their U.S. taxpayer clients to evade U.S. tax obligations. Importantly, DOJ emphasized that Julius Baer received substantial cooperation credit for its "swift and robust" internal investigation, the "continuous flow of unvarnished facts" to U.S. authorities, and for encouraging the two client advisors to accept individual responsibility for their misconduct, a clear nod to the Yates Memo principles discussed below. And, in March, the USAO announced that two subsidiaries of Cayman National Corporation -- Cayman National Securities and Cayman National Trust -- had agreed to plead guilty to conspiring with U.S. clients to hide more than $130 million in offshore accounts and evading taxes on income earned in such accounts, principally through the establishment and maintenance of sham Cayman corporations and trusts, The Cayman National subsidiaries also agreed to pay $6 million in disgorgement, restitution and a criminal fine and to provide ongoing cooperation. The USAO emphasized that the case represented the first convictions of financial institutions outside of Switzerland on cross-border tax evasion charges, underscoring DOJ's oft repeated promise to follow the money trail wherever it may lead.

The IRS reached its own cross-border tax enforcement milestone, announcing in October 2016 that more than 100,000 U.S. taxpayers had participated in the IRS's various offshore voluntary compliance programs implemented since 2008, resulting in the collection of more than $10 billion in back taxes, interest and penalties. As with the Swiss Bank Program NPAs, the IRS's offshore compliance programs are another source of substantial information from which U.S. authorities continue to develop new investigative leads.

Against this backdrop of continued aggressive enforcement activity by U.S. authorities, it is important for foreign financial institutions to maintain effective account due diligence programs for new and existing accounts to identify and document accounts in which U.S. persons hold a direct or indirect financial interest. Such programs help to ensure that foreign financial institutions can comply with applicable reporting requirements for such accounts and are in position promptly to take appropriate remedial steps to the extent necessary.

C. **FCPA Enforcement**

Last year, we cautioned against taking too much comfort from the declining number of cases brought by DOJ and the SEC in 2015 and the lack of any blockbuster fines. 2016 proved that this caution was indeed warranted as the number of resolved cases ticked up significantly, and there were several resolutions that rank among the largest FCPA fines of all time. Among them:

- In the largest ever global foreign bribery resolution, Brazil's Odebrecht S.A. and Braskem S.A agreed to plead guilty to conspiracy to violate the anti-bribery provisions of the FCPA and to pay a combined penalty of at least $3.5 billion to resolve charges in the U.S., Brazil and Switzerland arising out of a massive, global bribery and bid-rigging scheme (Dec. 21, 2016); notably, DOJ will receive only a small portion of the penalty, while the major part of the penalty will be shared between Brazil and Switzerland;

- Teva Pharmaceutical's agreement to resolve criminal and civil charges with DOJ and the SEC in connection with schemes to bribe public officials in Russia, Ukraine and Mexico, including criminal and civil payments totaling nearly $520 million, the largest FCPA resolution for a pharmaceutical company (December 22, 2016);

- JPMorgan's payment of a total of $264.4 million to resolve criminal and civil charges with DOJ ($72 million), SEC ($130.5 million) and the Federal Reserve Board ($61.9 million) in connection with conduct by its Hong Kong-based subsidiary to hire relatives and friends of Chinese government officials in an

effort to gain advantages in competing for banking business (November 17, 2016);

- Embraer's payment of a total of $225 million to resolve criminal and civil charges in the U.S. ($107 million to the DOJ and $98.2 million to the SEC) and Brazil ($20 million to Brazilian authorities) arising out of bribery of government officials in the Dominican Republic, Saudi Arabia and Mozambique, and the false recording payments in India via a sham agency agreement (Oct. 24, 2016);

- Och-Ziff's agreement to pay a total of $412 million to resolve criminal and civil charges with DOJ ($213 million) and the SEC ($199 million) arising out of bribes paid to public officials in the Democratic Republic of Congo and Libya. The firm's founder and chief executive also agreed to pay $2.2 million to settle books-and-records violations with the SEC (September 29, 2016); and

- VimpelCom Ltd and Unitel's resolution with DOJ and the SEC in which the companies admitted to a conspiracy to make more than $114 million in bribe payments in Uzbekistan and agreed to pay at least $795 million in criminal and civil penalties and disgorgement (February 18, 2016).

For several years we have emphasized that along with the "stick" of criminal charges, large fines and the imposition of monitors, DOJ and the SEC needed to improve the "carrot" by increasing the use of NPAs and even declinations. We were thus pleased to see the announcement in April of 2016 of the FCPA Pilot Program (DOJ Announces Pilot Program to Encourage FCPA Self-Disclosures) which, while it did not necessarily go as far as the business community might have wanted, was a potentially promising development. This one-year program for the first time, spelled out specific incentives for corporations that self-disclose FCPA misconduct and otherwise meet the "stringent" requirements of the program.

Since April when the Pilot Program was announced, DOJ has publicly declined prosecution under the FCPA in five cases: three in June 2016 involving Nortek, Inc., Akamai Technologies, Inc., and Johnson Controls, Inc., and two on

September 29, 2016 involving NCH Corp. and HMT LLC. Consistent with the Pilot Program requirements, the DOJ declination letters specify that each company had voluntarily disclosed the misconduct, conducted a "thorough" investigation, provided "full" cooperation (including identifying the individuals involved in the misconduct), undertaken remediation (including terminating the employment of the responsible individuals), and had enhanced (or were enhancing) both compliance programs and accounting controls to prevent a recurrence. Each declination letter also disclosed that the company would be disgorging profits realized from the illegal behavior. In the Nortek and Akamai Technologies cases, disgorgement and prejudgment interest were addressed in an NPA each company entered into with the SEC; Johnson Controls settled an administrative proceeding with the SEC which included a total payment of approximately $14.3 million covering civil penalties, disgorgement and prejudgment interest. In the HMT and NCH cases, both of which involved privately held firms, the amount of disgorgement was specified in the DOJ declination letter.

FCPA enforcement activity in 2016 shows that designing and implementing a strong anti-corruption compliance program remains as important as ever. While President-elect Trump has openly questioned whether strong FCPA enforcement impedes American businesses overseas, enforcement activity in 2016 also reinforces that anti-corruption enforcement is not just about U.S. authorities anymore. After years of DOJ and the SEC building up enforcement resources and also promoting strong anti-corruption laws and enforcement with government partners around the world, companies doing business internationally will continue to face FCPA and other anti-corruption enforcement risk in 2017 and would be wise to address it. As noted above, however, one way to appropriately alleviate the burdens on deserving companies is the amendment of the FCPA to include a compliance defense that would offer protection to those responsible companies that have made conscientious and extensive efforts to properly educate their employees and police against rogue employees who act in disregard of established company policy.

Rising Importance of State Attorneys General

The steady and consistent rise in the level of federal regulatory and enforcement activity over the past several years may well flatten or even change direction under the new Administration. However, companies should not assume that the overall number of investigations will decrease in 2017. Instead, any

decrease in federal activity may well be met by an increase in state attorneys general seeking to fill that perceived enforcement vacuum.

This would not be a surprising development. As has been often noted, in most states, the Attorney General is an elected position and many of the historically most active state AG offices currently are led by Democrats. For instance, the New York, California and Massachusetts AGs have been aggressively pursuing corporate investigations for years, with Democrats holding those three positions. Many state AGs have already expressed their intentions to be vigilant:

- Representative Xavier Bacerra, California's next Attorney General, stated that, "We'll look at the Constitution of the United States, and we'll look at our California constitution and recognize that as any other states, we will do whatever the U.S. Constitution allows us to do to protect our people and advance our interests."

- Eric Schneiderman, New York's Attorney General, has stated on numerous occasions that his office "stands ready to act to protect New Yorkers" regardless of whether his office finds allies in the future federal government and "will remain focused on rooting out fraud in financial markets, protecting consumers, and ensuring equal protection under the law for all New Yorkers."

Moreover, state AGs have already been pushing beyond the current bounds of federal enforcement activity in certain areas -- *e.g.*, insider trading and climate change. For example, the New York State Attorney General's settlement with BlackRock in 2014 suggests that the office may seek to use New York's Martin Act to extend beyond the scope of the federal insider trading laws. In that investigation, the NYAG alleged that BlackRock's surveys of Wall Street research analysts, which included questions about the companies they covered, gave BlackRock an unfair advantage over other market participants in violation of the Martin Act. The NYAG never alleged that BlackRock obtained any material nonpublic information, but simply alleged that BlackRock obtained nonpublic opinions about certain companies, which gave BlackRock an unfair informational advantage in its trading activities. Similarly, the NYAG and Mass AG offices are

currently pursuing well publicized investigations regarding climate change and environmental disclosures involving ExxonMobil, among other companies.

State AG-led investigations can be particularly burdensome on companies for a variety of reasons. First, the fact that an issue has traditionally been the subject only of federal regulation—for instance, federal securities law disclosure—does not necessarily prevent a state AG from pursuing that issue. Second, state AGs often work together and large companies may face potential multi-state investigations pursued in concert by multiple states' attorneys general. While the potential monetary and punitive consequences of one state's investigation can be a significant challenge, a company's exposure is exacerbated when dealing with multiple states' laws and forums.

ExxonMobil is currently seeking to block such non-federal activity. The company brought a federal action in Texas to block the Mass AG and NYAG climate change probes on the ground that they are an impermissible attack on ExxonMobil's free speech rights. ExxonMobil had some initial success—in November 2016, the federal district court issued an order requiring Massachusetts AG Maura Healey to give a deposition on December 13 and requiring New York AG Eric Schneiderman to be available on the same day. However, on the day prior to Healey's deposition, the court canceled her deposition and ordered the parties to submit briefing addressing the issue of whether the court has personal jurisdiction over Healey and Schneiderman. The court has since stayed all discovery, and the jurisdictional issue remains unresolved. Thus, it will be important to continue to monitor this case, which may serve as a bellwether of federal courts' willingness to limit investigations by state attorneys general.

The Yates Memo

It is slightly more than a year since DOJ promulgated the "Yates Memo," designed to focus prosecutors' efforts on pursuing individuals responsible for corporate wrongdoing and to encourage corporations to provide evidence of wrongdoing by corporate actors. Deputy Attorney General Sally Yates noted in a recent valedictory that it is too early to assess the impact of the Memo. This assessment seems fair, as very few, if any, investigations commenced after the Memo was issued have as yet resulted in charges, and it is accordingly premature to measure the impact on actual prosecutions.

But it is clear that the Memo has resulted in prosecutors taking longer looks at the potential culpability of corporate employees, in some cases prolonging already extensive investigations. A related effect has been that separate counsel are more frequently being retained on behalf of corporate employees as it is more difficult for counsel to represent both the corporation and an individual given the increased potential of individual exposure. Clearly, the heightened focus on individual responsibility is not designed to supplant aggressive focus on corporate conduct. DAG Yates expects that "when companies enter into high-dollar resolutions with the Justice Department, you'll see a higher percentage of those cases accompanied by criminal or civil actions against the responsible individuals."

As DAG Yates also recently noted, the incoming Administration has not expressed a view on the policies underlying the Memo. Given the populist themes of the past election season, the apparently widely-held view that pursuing culpable individuals is sensible policy, and the obstacles to changing course in an agency as large as DOJ, it seems unlikely that in the near-term there will be substantial change in the DOJ focus on individual responsibility.

Ultimately, much of the disparity in the prosecution of corporations and individuals is a consequence of differing incentives. Corporations generally face significant collateral consequences arising from criminal charges and trials, and in most situations have substantial incentives to resolve investigations via settlement, even in complex or close cases. Individuals, faced with prison or bankrupting fines, have strong incentives to put DOJ to its proof, and prosecutors are understandably reluctant to pursue cases where the evidence of individual culpability (particularly as to *mens rea*) is questionable. It remains to be seen whether the change in policy expressed in the Yates Memo will meaningfully change these forces as 2017 unfolds.

SEC Developments

Wide-ranging changes in the leadership of the SEC are underway. President-elect Trump has nominated corporate lawyer Jay Clayton to succeed Mary Jo White. The timetable for the Senate to consider this nomination is not yet clear. With two other seats already vacant, Chair White's departure will leave only two Commissioners in office, Republican Michael Piwowar and Democrat Kara Stein, until the vacancies are filled. In addition, a growing number of senior staff have departed the agency in recent weeks or announced plans to do so.

During the interim period in which there is a two-member Commission, each Commissioner will in effect have veto power, as a majority vote is required to approve any staff recommendation. Thus, either Commissioner will have the ability unilaterally to block the commencement or settlement of an enforcement action, or the initiation or adoption of a rule-making proposal. There is no reason to expect disruption of mainstream enforcement or regulatory activities. But the Commission is unlikely even to consider controversial matters during this interim period.

Much of the Commission's enforcement docket is likely to be unaffected by the change of administration. Political considerations do not come into play when the Commission is considering an egregious accounting fraud, a clear-cut insider trading case or a Ponzi-scheme offering fraud. Some of the innovations of recent years have been widely viewed as successful, and may well be retained under a new administration. For example, the national investigative units have lived up to the goal of developing specialized expertise and a store of knowledge and experience.

Probably the most prized innovation within the SEC is the whistleblower bounty program that was mandated by Dodd-Frank and has now been in operation for five years. The Commission continues to promote the whistleblower program and highlight its contributions to the agency's enforcement efforts. In fiscal 2016, the SEC received 4,218 whistleblower reports, the most since the program's inception. Over the five-year period, the SEC has awarded a total of over $111 million to 34 whistleblowers. The SEC distributed over half of that money in fiscal 2016, including its second- and third-highest awards ever, in the amounts of $22 million and $17 million respectively. The Commission also continued its efforts to support whistleblower protections through enforcement action. The Commission brought its first stand-alone whistleblower retaliation case in September, against a company that was not charged with any substantive violations of the securities laws. The Commission also brought a series of cases over the course of the year involving provisions in severance agreements that could be read as prohibiting whistleblowing activity in violation of Rule 21F-17(a). There is every reason to expect the whistleblower program to continue to be an important source of investigative leads. Corporate disclosure and financial reporting continues to be the largest category of whistleblower reports coming in to the SEC, as it has been since the inception of the program.

One area of recent innovation that may draw the attention of the new administration is the increasing "criminalization" of the SEC's civil enforcement process. A prime example of this is the relatively new policy of requiring admissions from companies seeking to settle certain enforcement actions. For decades, the Commission effectively communicated its enforcement messages by means of no admit/no deny settlements, and it largely continues to do so even today. Indeed, the no admit/no deny approach enables companies to sign on to settlements that they might be unwilling to accept if admissions were required, thus facilitating the Commission's ability to vindicate its enforcement interests. By contrast, a company that enters into a settlement that includes admissions must accept the potential of significant collateral consequences.

In its year-end report on its enforcement program, the Commission highlighted the cases below, in which it obtained admissions. In none of these cases is there any discernible basis to conclude that exacting admissions communicated an enforcement message or served a public interest that was not already fully addressed by the charges brought, the penalties assessed and factual findings that could have been made on a no admit/no deny basis. Nor do the cases suggest that the Commission has deployed the admissions "weapon" in cases of the most egregious frauds or the most severe injury to investors:

- *In the Matter of Citigroup Global Markets, Inc.* (July 12, 2016) involved violations of recordkeeping requirements due to a computer coding error. The settlement included a $7 million penalty.

- *In the Matter of Grant Thornton, LLP* (Dec. 2, 2015) was a case of audit failure by a public accounting firm. Grant Thornton made admissions and paid a $3 million penalty as well as $1.5 million in disgorgement of audit fees plus prejudgment interest. The SEC also simultaneously settled an enforcement action against the two responsible audit partners, who were suspended from practicing before the SEC, but did not make admissions.

- *In the Matter of JPMorgan Chase Bank, N.A.* (Dec. 18, 2015) involved failures by investment advisory businesses to disclose certain conflicts of interest, such as a preference for investing in proprietary products in managed accounts. The relevant

affiliated entities paid a $127.5 million penalty plus $139.315 million in disgorgement and prejudgment interest.

- *In the Matter of Barclays Capital Inc.* (Jan. 31, 2016) involved regulatory violations and misrepresentations concerning features of a "dark pool" alternative trading system. Barclays paid a $35 million penalty. On the same day, the SEC announced a similar case against another bank, which included a $30 million penalty plus $24.3 million in disgorgement and prejudgment interest, but no admissions.

- *In the Matter of Ethiopian Electric Power* (June 8, 2016) addressed an unregistered offering of bonds by a foreign government-owned utility, where no exemption from registration was available. The foreign issuer paid $6.5 million in disgorgement and prejudgment interest.

- *In the Matter of Merrill Lynch, Pierce, Fenner & Smith Inc.* (June 23, 2016) involved violations by a broker-dealer of rules relating to the safekeeping of customer cash and securities. The settlement included a $358 million penalty plus $57 million in disgorgement and prejudgment interest.

At its inception, the admissions policy was a solution in search of a problem. In practice, it is difficult to see that the policy has served a public policy interest that the Commission is not already addressing fully through the no admit/no deny settlements that it continues to obtain in most of its cases. The change of administration at the SEC may present an opportunity to revisit the question of whether this innovation has in fact enhanced the enforcement program.

John F. Savarese	Ralph M. Levene
Wayne M. Carlin	David B. Anders
Jonathan M. Moses	Marshall L. Miller
Louis J. Barash	Carol Miller