January 30, 2020

White-Collar and Regulatory Enforcement: What Mattered in 2019 and What to Expect in 2020

Introduction

The main takeaway from white-collar and regulatory enforcement activity in 2019, which we believe will remain true through 2020, is that both the DOJ and SEC have become more transparent about the requirements for receiving corporate cooperation credit. Last year’s experience shows that the government’s pronouncements about the credit it will extend to exemplary companies are not mere window-dressing, but are instead backed up with significant reductions in fine and penalty amounts, as well as outright declinations in cases where a company satisfies the government’s stated expectations concerning self-detection, self-reporting, cooperation and remediation.

Cases brought against individual corporate officers also continued apace in 2019, in keeping with the government’s oft-stated commitment to ensuring that individual wrongdoers, and not just their corporate employers, are held responsible. Indeed, last month, Assistant Attorney General Benczkowski stressed that “[s]o far this year, the Fraud Section has brought charges against more than 440 individuals, which is an all-time high that will only increase through the close of the year.” One consequence of this trend, as we discuss below, is that because individuals frequently take cases to trial, unlike corporations which almost always settle, the government has suffered some high-profile losses. We expect this trend to continue in 2020.

State attorneys general likewise remain very active across a broad range of subject matter areas — from investigations prompted by the opioid crisis, to attempts to recover costs associated with climate change, concerns about vaping and youth addiction, environmental law enforcement, and data privacy. These investigations, as we also discuss, can prove challenging for companies because law-enforcement priorities, settlement opportunities and political objectives can vary widely from state to state.

While the overall scale of criminal fines and penalties imposed by DOJ in 2019 has dropped from the peak years following the 2008-09 financial crisis and the ensuing massive investigations of financial institutions, there is no question that white-collar criminal and regulatory enforcement remains active and
robust. For example, more than $2.8 billion in corporate penalties were levied last year in FCPA enforcement cases, the highest level ever in that area, and, overall, the DOJ secured nearly $8 billion in total monetary recoveries through resolutions of corporate criminal investigations in 2019. The lesson is that well-managed companies must remain vigilant and well-prepared in the event of a compliance problem. But the good news is that if a corporation maintains an effective compliance regime that periodically reassesses the company’s risk profile, refreshes its policies and procedures accordingly, carries out well-designed training programs, encourages the surfacing by employees of potential compliance issues, ensures that self-reporting is carefully and appropriately considered, provides thorough and effective cooperation if an issue does surface, and engages in timely and comprehensive remediation, then a successful outcome (involving substantial fine reductions, if not an outright declination) is achievable. We have seen this in action in several major cases we handled last year.

DOJ Developments

In the third year of the Trump Administration, DOJ appears to have found its stride. Last year, we highlighted policy changes that DOJ had undertaken — focusing primarily on bringing much-needed transparency to companies under investigation — as well as DOJ’s focus on individual accountability. Over the past year, DOJ’s implementation of these new policies provides helpful insight into the government’s evolving approach to criminal enforcement in the white collar context.

Transparency. DOJ has made an effort to be more transparent about its charging decisions and the specific benefits it will extend to companies that provide complete cooperation. Among other things, DOJ’s FCPA Corporate Enforcement Policy, which has been in place since 2017, sets forth criteria for voluntary self-disclosure, cooperation, and remediation that, if satisfied, create a “presumption” of declination of criminal enforcement action, as well as aggravating factors that cut against a declination. DOJ also announced updated guidance for prosecutors, identifying factors used to evaluate corporate compliance programs when considering corporate resolutions. Assistant Attorney General Benczkowski stressed in a recent speech that “it is not in the Criminal Division’s interest to be opaque about the factors we want our prosecutors to consider when evaluating corporate compliance programs. We want the corporate community to invest heavily in compliance, and do so efficiently and effectively.”

Individual Accountability. Individual accountability has been a consistent DOJ theme and enforcement priority, and 2019 was no exception.
Indeed, DOJ’s strategy of providing meaningful incentives to corporations for their cooperation, including disclosing information about individuals substantially responsible for corporate misconduct, has helped DOJ gather evidence necessary for effective prosecutions of individuals, an often resource-intensive endeavor. The upshot of this individual-focused approach is that DOJ has been involved in more trials, engendering more jurisprudence refining the contours of our nation’s criminal laws.

Successful prosecutions of high-level corporate executives include the (i) former chief executive officer of PixarBio, who was convicted for investor fraud and obstructing an SEC investigation, (ii) former chief executive officer of Yukom Communications Ltd, who was charged with a scheme to market binary options to investors, and (iii) three former Credit Suisse bankers who pleaded guilty to involvement in a $2 billion fraudulent loan scheme in Mozambique. But the government also suffered some significant losses. For example, a federal judge in Northern California acquitted a former Barclays FX trader by granting a directed verdict for him on charges of engaging in an FX manipulation scheme. Then, in Platinum Partners, a New York federal judge took the unusual step of overturning a conviction, finding there was insufficient evidence of criminal intent. Similarly, late in 2019, a Brooklyn jury acquitted a shipbuilding executive in connection with the aforementioned $2 billion fraudulent loan scheme in Mozambique.

Notwithstanding these losses, AAG Benczkowski has made clear that DOJ’s focus on individuals is likely to continue into 2020. As he stated in December, the high “number of individual prosecutions in 2019 is not an outlier or a statistical anomaly. Rather, it is part of the Department’s continued dedication to holding individual wrongdoers accountable across the board.”

**Insider trading**

Insider trading continues to be a major enforcement focus, with particular attention paid this year to international activity. The government won a conviction against Telemaque Lavidas, a U.S. resident alleged to have tipped non-U.S. persons about events in a pharmaceutical company on which his father sat on the board. A key witness in the trial was a Swiss-based trader who was arrested in and extradited from Serbia, pleaded guilty and cooperated with the government. Other members of the alleged conspiracy have been indicted but remain at large. The government’s aggressive efforts in this and similar matters provides a clear warning that international borders will not be a protection against prosecution for insider trading on U.S. markets.
Perhaps the most significant development in this area was the late December ruling by the Second Circuit Court of Appeals in *United States v. Blaszczak*, holding that the Dirks and Newman requirement of a personal benefit did not apply to insider trading prosecutions under the wire fraud statute and the criminal securities law statute added to Title 18 by the Sarbanes-Oxley Act of 2002. In *Blaszczak*, the jury acquitted the defendants of insider trading charges under section 10-b of the Exchange Act (Title 15), but convicted on the Title 18 counts. The Second Circuit held that the element of a personal benefit was a judge-made doctrine unique to the relevant securities law provisions and that the same requirement should not be grafted onto the Title 18 provisions. The court also held that the inside information in that case — concerning upcoming FDA regulatory rulings — constituted “property” in the hands of the government for purposes of the Title 18 fraud statutes.

The *Blaszczak* holding likely will increase the complexity of advising on insider trading matters. Given Freedom of Information Act requirements and other open government initiatives, it may be difficult to determine whether information other than classified information or other items expressly identified as secret are government property that is susceptible of being misappropriated for personal use and gain.

The impact of the court’s personal benefit holding is harder to predict. Prosecutors have at times found it difficult to establish a personal benefit in situations in which a friend or acquaintance divulges information for no immediate or obvious benefit. Because prosecutors are likely to charge cases in those circumstances using the *Blaszczak* precedent under Title 18, other Circuits and the Supreme Court may ultimately have occasion to revisit the viability of that approach.

**Spoofing**

DOJ and the CFTC have made enforcement against marketplace spoofing a significant priority. DOJ’s Fraud Section pursued a number of spoofing cases, primarily in the Northern District of Illinois (where the major commodity exchanges are located) and the prosecutions have been aggressive, including a case brought in August of last year in which spoofing was charged as a RICO conspiracy.

Marketplace spoofing — not to be confused with the ubiquitous and annoying practice of email spoofing, in which malicious emails are sent disguised to look as if they come from frequent and respected email senders — is defined as
placing an order that one does not intend to execute. Spoofing was expressly proscribed in the commodities markets by a provision in the 2010 Dodd-Frank law. While that provision is limited to the commodities markets, in a key ruling in October 2019, the District Court for the Northern District of Illinois held that spoofing also satisfies the elements of wire fraud. Under that holding, spoofing in securities markets is a federal felony.

Spoofing is designed to have an order or series of orders placed and then quickly withdrawn in an effort to affect the market, thereby allowing the trader to execute a subsequent order at a favorable price. Thus, the key element in a spoofing case turns on whether the trader actually intended the initial order to be executed. In one of the first spoofing cases to reach an appellate court, the Seventh Circuit upheld the trader’s conviction, finding that the trader sought to create a trading algorithm that avoided the execution of all orders. The court did not find persuasive that some of the orders were in fact executed.

The government suffered some early setbacks in its spoofing prosecutions, with an acquittal in the 2018 Flotron case in Connecticut and a hung jury (and subsequent voluntary dismissal) in the Thakkar case in Illinois in early 2019. But the government has also had some recent successes, including criminal settlements with at least four traders and a significant criminal settlement with one of their trading firms, and rejections of defense motions to dismiss in two N.D. Illinois cases. It seems likely that the government’s aggressive pursuit of spoofing will continue in 2020, although that strategy could be affected by the results in several major trials likely to take place over the course of this year.

Firms’ compliance efforts in the spoofing area should include computer programs or other procedures to identify large withdrawn orders with nearly simultaneous executions on the contra side of the market and prompt supervisory and compliance attention to such situations to identify the reason for the withdrawn orders. This is no small task; given the huge volume of orders in the electronic age, such oversight is likely to be time-consuming and expensive.

SEC Developments

In 2019, the SEC largely continued to pursue the same enforcement priorities that have been at the top of the agency’s agenda throughout the tenure of Chairman Jay Clayton. Through its public statements, allocation of resources and cases brought, the SEC has continued to press investigations of schemes targeting “Main Street” or retail investors. Underscoring this focus, the SEC issued rules, known as the “Best Interest” rules, to make clearer the obligations of financial
advisors to serve the best interests of their customers. These “Reg BI” rules will go into effect this year. Other key priorities were cyber-related investigations and cases against individuals responsible for wrongdoing in a corporate setting.

In reviewing the statistical profile of the SEC’s enforcement activity in fiscal 2019, it is worth keeping in mind that the agency experienced a 35-day lapse in appropriations early in the calendar year, during which nearly all investigative activity ground to a halt. Even with this significant interruption, the SEC brought a total of 526 standalone enforcement actions in 2019 (excluding follow-on administrative proceedings and delinquent filing cases) — an increase over the 490 such cases filed in 2018. The agency’s funding was eventually increased, enabling the SEC to lift a long-standing hiring freeze.

Cases against public companies involving accounting, financial reporting and disclosure violations have always been a mainstay of the enforcement program. In its annual report for 2019, the Division of Enforcement highlighted this area, and highlighted five cases brought against well-known companies in 2019, in which the Commission obtained penalties ranging from $15 million to $100 million. Cases of this type are complex and both resource-intensive and time-consuming; in 2019, they averaged 37 months from opening to filing.

The Division also highlighted a sixth accounting case that was completed in just 17 months, where the Commission imposed no penalty in recognition of the issuer’s “prompt self-reporting, extensive cooperation, and implementation of remedial measures immediately upon learning of the improper conduct for which it was charged.” In a parallel criminal investigation, the DOJ determined to take no action against the same company. We represented the issuer’s Audit Committee in this matter and conducted the internal investigation — everything that the company did was directed toward objectively learning the facts, remedying the problem and facilitating the completion of governmental investigations. The result shows that both the SEC and DOJ are genuinely willing to recognize and reward exemplary cooperation. The SEC’s publicly stated desire to speed up complex investigations also creates opportunities for companies willing to take the steps necessary to demonstrate that they are good corporate citizens.

The whistleblower program remains an important component of the SEC’s enforcement arsenal. The agency received 5,212 reports in 2019, a slight decline from the 5,282 reports received in 2018. This small dip was the first annual decline since the inception of the program in 2011. We see this merely as
an indication that the program has matured, with the number of tips stabilizing at a high level. In keeping with historical patterns, the single largest category of reports related to corporate disclosures and financial statements, while 200 complaints involved potential FCPA-related misconduct. In 2019, the SEC distributed a total of $60 million in awards to eight whistleblowers (down from the $168 million awarded to 13 whistleblowers in 2018). Again, we do not view these figures as indicating any decline in the significance of the whistleblower program — the number and amount of awards can be expected to vary depending on the flow of cases in the enforcement pipeline and the magnitude of recoveries obtained. Notably, in 2019 the SEC made its first award ($4.5 million) to a whistleblower who did not first contact the SEC, but instead received credit for reporting a matter internally, which prompted an internal investigation by the employer. The whistleblower’s report involved alleged FCPA misconduct and the employer — which media reports indicated was Zimmer Biomet Holdings — later reported its findings to the SEC and ultimately resolved DOJ and SEC FCPA investigations.

Finally, the SEC continues to grapple with the aftermath of the Supreme Court’s June 2017 decision in *Kokesh v. SEC*, which held that SEC claims for disgorgement are “penalties” subject to a five-year statute of limitations. *Kokesh* expressly did not address the question whether the SEC has authority to seek disgorgement in injunctive actions. The Court granted certiorari to consider that issue in *Liu v. SEC*. An adverse decision would remove an important element of relief that the SEC seeks whenever a defendant has obtained monetary gains from alleged wrongdoing. The outcome in *Liu* will not affect administrative proceedings, where the SEC has express statutory authority to obtain disgorgement. Thus a loss in the Supreme Court would likely lead the SEC to bring more settled cases administratively, and might affect the SEC’s choice of forum in litigated cases where disgorgement may be an appropriate remedy.

**State Attorneys General**

Consistent with our past predictions, state attorneys general brought an increasing number of enforcement actions in 2019, particularly in traditional consumer protection areas. Opioids and e-cigarettes are subjects of intense scrutiny and we expect state AGs to continue taking action on these and other similar topics given pending investigations and public frustration with the federal government’s perceived inaction on these issues.

The complicated web of opioid litigation that we described last year remains pending. Discussions of a global settlement among state AGs and certain
pharmaceutical companies have been ongoing throughout 2019. The opioid litigation illustrates the challenge of coordinating multilateral settlement discussions with many state AGs, each of which have their own political considerations and litigation objectives.

State AGs also are beginning to turn their attention to the “e-cigarette” industry. AGs from a growing number of states are investigating companies like Juul Labs and its industry peers for potential violations of consumer protection laws and for advertising allegedly targeting minors. Several states, including New York, California, North Carolina, Massachusetts, and Arizona, brought suit last year against these companies. These cases are still in their early stages.

Besides these traditional consumer protection areas, we also saw substantial AG activity in the antitrust space. Though state AGs have traditionally been important partners to federal government regulators in the area of antitrust enforcement, in recent years state AGs have shown an increased appetite to pursue independent antitrust investigations and to seek remediation that is more demanding than that requested by the federal government. For example, the attorneys general of nearly every state in the country are coordinating investigations focusing on several tech giants — in particular, Google, Facebook, Amazon and Apple — for various violations of antitrust laws.

Climate change is another area outside the traditional scope of state AG efforts where we nonetheless saw increased AG attention this past year. At this stage, it is not clear whether the legal theories pursued by state AGs on this issue will be successful. New York State, for example, recently lost a bellwether lawsuit against Exxon for allegedly making fraudulent statements concerning its accounting for costs associated with climate change regulation. This case may demonstrate to state AGs the challenges inherent in pursuing novel legal theories as a mechanism to promote public policy goals. Nevertheless, various states and municipalities continue to pursue lawsuits against oil and gas companies in an effort to recover costs alleged to be associated with climate change. Those cases merit attention in the coming year.

State AG investigations and lawsuits can present unique problems for corporations. The diversity and breadth of state AGs make it hard to navigate multiple concurrent investigations and to reach uniform resolutions, as each state AG may face unique political considerations and constraints relevant to his or her state (as reflected in the opioid cases). As a result, companies can face a patchwork of negotiations, which, if not carefully coordinated, can lead to long-
term legal problems for companies, even those willing to engage in settlement discussions.

**FCPA Enforcement**

By all accounts, 2019 was a very active year in FCPA enforcement. The DOJ and SEC resolved a combined total of 14 corporate cases, imposing more than $2.8 billion in fines, disgorgement and interest. The corporate resolutions included two of the largest FCPA settlements ever — the $1.06 billion joint DOJ/SEC resolution with Swedish telecom company Ericsson for misconduct spanning multiple countries, and the $850 million joint DOJ/SEC resolution with Russian mobile telecom company Mobile Telesystems, which was the third major FCPA settlement arising out of a long-running bribery scheme involving the daughter of the former president of Uzbekistan in return for assistance in entering and continuing to operate in the Uzbek telecom market. Consistent with the DOJ’s 2018 Policy on Coordination of Corporate Resolution Penalties, the Mobile Telesystems resolution included credit for the civil penalty imposed by the SEC.

Corporate resolutions involved a wide-range of industries — including healthcare/medical, telecom, information technology, financial services/banking, consumer retail and energy/natural resources — and a similarly wide-range of countries and regions — including China, Mexico, Brazil, India, Hungary, Saudi Arabia, Egypt, Morocco and Angola. Corporate resolutions also reflected long-standing efforts by U.S. authorities to work with law enforcement authorities in other jurisdictions, including Brazil, France, Switzerland, the U.K. and Sweden, and two of 2019’s corporate resolutions included substantial DOJ credit for fines to be paid to foreign authorities.

DOJ also issued two public declination letters (Quad/Graphics; Cognizant Technology) pursuant to its FCPA Corporate Enforcement Policy, and several other companies reported that previously disclosed FCPA DOJ and/or SEC investigations were closed by DOJ without any charges being brought although no formal declination letter or other resolution was made public. Indeed, this trend continued into 2020, as Uber reported on January 6th that DOJ closed an FCPA inquiry dating back to 2017 without any charges being brought although, here again, no declination letter was made public.

Making good on promises to hold individuals accountable, the DOJ and SEC in 2019 vigorously pursued charges against individuals responsible for FCPA misconduct. DOJ announced FCPA-related charges against more than
twenty individuals in 2019, many of which resulted in guilty pleas. The SEC initiated six FCPA-related individual cases, three of which were resolved in 2019.

Perhaps more significant, in three separate trials, DOJ obtained convictions against four individuals charged with FCPA misconduct. In one of those cases, involving British national and former Alstom S.A. executive Lawrence Hoskins, the Second Circuit had previously ruled (United States v. Hoskins) that a foreign national not acting within U.S. territory in connection with a foreign bribery scheme — a jurisdictional requirement for FCPA liability — may not be charged with conspiracy or aiding and abetting an FCPA violation. The Court, however, left open the possibility of liability if a foreign national acting only abroad did so as an “agent” of an entity otherwise subject to FCPA jurisdiction. At trial last year, DOJ succeeded on that alternative theory, demonstrating that Hoskins acted as an agent of Alstom’s U.S. subsidiary based on his central role in carrying out the bribery scheme from which it benefitted, even though under Alstom’s formal corporate structure Hoskins worked for the French parent company, not the U.S. subsidiary. It remains to be seen whether this “agency” approach will prove successful in future cases with varying fact patterns.

DOJ’s declination letter to Cognizant Technology Solutions also answered the question of how the FCPA Corporate Enforcement Policy’s declination presumption would hold up in a case involving significant aggravating factors. Even though the company’s then-President and Chief Legal Officer were directly involved in authorizing the bribe and took steps to conceal their conduct, DOJ nevertheless declined to charge the company itself based on its exemplary efforts, including voluntary self-disclosure within two weeks of the company’s board learning of the misconduct, thorough internal investigation, proactive cooperation, and the existence of an effective compliance program.

At the other end of the spectrum, German medical products and services company Fresenius Medical Care resolved a DOJ FCPA investigation through an NPA that included a criminal penalty of $84.7 million and imposition of an independent compliance monitor for two years, even though the company self-reported the misconduct pursuant to the FCPA Corporate Enforcement Policy. In explaining its decision, DOJ highlighted the company’s failure to timely and fully respond to certain DOJ requests, the breadth of the misconduct (spanning 13 countries), and concerns about the effectiveness of the company’s compliance program.
Cybersecurity Developments

While the internet has continued to be an enormous driver of innovation and efficiency in the corporate world, it also exposes companies to tremendous risks. Breaches at entities as technologically advanced as Yahoo! and Facebook, and as large as the U.S. government, have shown that no system is immune from attack. Given nearly universal reliance on the internet, almost all companies today face data privacy risk, cybersecurity risk, or both. 2019 was replete with examples of how these risks can arise. Taking just two examples:

- Facebook agreed to a $5 billion penalty and extensive remedial requirements to resolve an investigation into violations of a 2012 consent decree related to its data privacy practices. The monetary penalty of $5 billion dwarfs all prior fines in this area. Further, the remedial order imposes expansive compliance obligations and vigorous accountability and reporting requirements, including the establishment of a board privacy committee made up of independent directors, designation of compliance officers accountable to that committee, a third-party compliance assessor with enhanced authority and independence, heightened privacy requirements for sensitive applications and activities, and quarterly privacy certifications to the FTC, including from the CEO.

- Capital One faced a significant data breach, exposing more than 100 million customer accounts in the U.S. and another 6 million in Canada. While the magnitude of the breach was significant, Capital One’s existing policies and rapid response enabled it to contain a substantial amount of the potential damage, thereby distinguishing the event from some prior incidents in the industry. On July 29, 2019, Capital One announced it had determined that a single individual formerly employed by a vendor had obtained unauthorized access to its systems and to stored personal information concerning credit card products and credit card customers. The breach occurred in March 2019, and Capital One discovered the incident in response to a report by an external security researcher on July 17, 2019 submitted through Capital One’s Responsible Disclosure Program. Cybersecurity observers commented favorably on both the disclosure program and the speed of the bank’s response, which contributed to the prompt arrest of the hacker by the FBI. Though the program enabled the bank to identify and remedy the vulnerability in their system, it did not prevent the predictable litigation fallout, including private consumer class action cases in the U.S. and Canada, a federal securities class action, and governmental inquiries.
Keeping pace with evolving cyber threats, regulatory oversight remains active and ever-changing. At the federal level, both the FTC and the SEC are focused on cybersecurity and data privacy. The Facebook resolution discussed above was one of many FTC enforcement actions announced or resolved in 2019, in line with its intense focus on data security issues. More recently, on January 27, 2020, the SEC Office of Compliance Inspections and Examinations published new observations on cybersecurity and resiliency practices. Other federal regulators are active, particularly in industries where companies are likely to possess large quantities of sensitive personal data. For example, HHS, which regulates patient privacy under the Health Insurance Portability and Accountability Act (HIPAA), has amassed record penalties in the past few years for privacy breaches under HIPAA including a $16 million settlement with Anthem Inc. concerning a breach exposing data of almost 79 million people. State AGs also remain active in this area. Taking just one example, in July 2019, a coalition of 50 AGs announced that a settlement had been reached with Equifax stemming from the company’s famous 2017 data breach, with Equifax paying up to $600 million with $175 million going to the states.

2019 also saw the continued impact of the European Union’s General Data Protection Regulation (GDPR) on global cybersecurity and data privacy practices, including on U.S.-based multinationals. Among other things, this law requires entities storing personal data of E.U. nationals to obtain express and specific consent for the processing of such data — consent which can be subject to withdrawal. The GDPR also empowers the data subject to demand erasure or correction of personal data. This legislation has bite: last January, Google was the subject of France’s first significant enforcement action under the GDPR, paying a €50 million penalty for violating the law’s transparency and consent obligations.

California has gone even farther. As we have noted, the California Consumer Privacy Act (CCPA) became effective on January 1, 2020, and imposes unprecedented obligations relating to data privacy on companies that transact business in the state, defined to potentially include a sweeping number of out of state companies, requiring increased data use transparency and the observance of novel consumer data rights (including the right to opt out of the sale of personal information).

Under the CCPA, the California AG can impose fines including damages up to $7,500 for each intentional violation (and $2,500 for each unintentional violation), if not cured within 30 days. In addition, the CCPA provides consumers with a private right of action. Just as we saw significant enforcement penalties in the first year following the adoption of the GDPR, we
expect the CCPA to similarly produce adverse consequences for companies not adequately responding to the evolving requirements of cybersecurity.

**Conclusion**

While their priorities are evolving, federal authorities and numerous state governments continue to aggressively prosecute white collar crime. Importantly, the “carrot” extended to companies that self-disclose, cooperate, remediate and maintain effective compliance programs is bigger than ever before, but so too is the “stick” used by DOJ and other prosecutors when companies fall short of the government’s expectations in this new era of transparency.

Attention to compliance thus remains mission critical. Reinforcing the government’s prescriptions, the well-known *Caremark* doctrine similarly counsels directors to take reasonable and well-designed steps to satisfy their duty of loyalty by exercising proper oversight. In a recent [opinion denying a motion to dismiss a Caremark claim](#), the Delaware Supreme Court explained that, “[w]hen a plaintiff can plead an inference that a board has undertaken no efforts to make sure it is informed of a compliance issue intrinsically critical to the company’s business operation, then that supports an inference that the board has not made the good faith effort that *Caremark* requires.” The careful design, implementation and periodic assessment of compliance systems to ensure they are up-to-date, appropriately tailored to the reputational, legal and regulatory risks faced by the company, and functioning effectively, are more important than ever.

John F. Savarese       Ralph M. Levene
Wayne M. Carlin        Jonathan M. Moses
David B. Anders        Louis J. Barash
Celia A. Glass         Tamara Livshiz
Carol Miller