TOPICS COVERED
// Strategy & Trends

AVOIDING BROKEN WINDOWS IN A GLOBAL CORPORATE HOUSEHOLD

Check-ups and regular monitoring are key to staying on track with your compliance policies

Written by John D Buretta

Corporate compliance programs have never been more important. The question today is not whether to have a compliance protocol, but whether the program in place has the agility to adapt to enhanced regulatory rulemaking, robust enforcement, and strategic corporate moves from new global partnerships and joint ventures to mergers and acquisitions.

In many ways, the regulatory landscape in which compliance teams now operate is more challenging than ever. During public statements over the past year, the Securities and Exchange Commission (SEC) has emphasized that it will pursue corporate wrongdoing ranging from the most serious to the smallest "broken window." While many recent corporate investigations have focused on traditional financial crimes such as insider trading, accounting fraud, consumer fraud, and market manipulation, the SEC's enforcement roster also includes smaller-scale rules enforcement, including delinquent securities filings. Added to these enforcement efforts is the SEC's recent activity in seeking to implement Dodd-Frank rules on a range of subjects from credit rating agencies to swaps. Once implemented, these rules may eventually pave the way for future avenues of securities enforcement.

Another active enforcement area is the array of criminal and civil enforcement statutes rooted in US foreign policy and national security interests: the Foreign Corrupt Practices Act (FCPA); the International Emergency Economic Powers Act and related sanctions laws; the Trading with the Enemy Act; the Arms Export Control Act; the International Traffic in Arms Regulations and related export controls; and the Bank Secrecy Act (BSA), as amended by the USA PATRIOT Act, along with related anti-money laundering requirements. Depending on the particular statute, numerous agencies today have investigative and enforcement authority: the Department of Justice; the Federal Bureau of Investigation; the SEC; the Department of the Treasury's Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN); the Department of Commerce's Bureau of Industry and Security (BIS); and the Department of State. Across the spectrum of potential offenses, there is unprecedented coordination among both domestic and foreign law enforcement agencies. It is unlikely that the current enforcement momentum will abate.

Anti-corruption initiatives, for example, remain a key US law enforcement priority. The monetary penalties imposed in FCPA-related cases are illustrative. Between 2002 and 2006, criminal and civil penalties for alleged FCPA violations by corporations totaled approximately $154 million. Between 2007 and 2013, more than $4.8 billion in FCPA-related penalties were assessed. The number of prosecutions of individuals for FCPA-related offenses has also increased, with nearly three times the number between 2008 and today than during the previous decade. In an evolving strategic approach, US federal prosecutors have also pursued a range of criminal charges in foreign bribery cases beyond the FCPA itself—including federal obstruction, money laundering, and Travel Act commercial bribery counts—and charged some defendants not traditionally encompassed by the FCPA, including foreign officials who are alleged to have accepted bribes. Outside the United States, anti-corruption enforcers in numerous countries are acting on new anti-corruption laws and devoting further resources to detecting and punishing bribery.

On the US sanctions front, OFAC continues rigorous enforcement of a spectrum of embargo-related laws, regulations and Executive Orders. Since 2009, OFAC settlements have more frequently reached into the hundreds of millions of dollars, with nearly $2.5 billion in penalties imposed during the past three years, including over $1.2 billion in penalties imposed so far this year alone. This increased enforcement activity comes at a time of renewed use of sanctions as a means to address geopolitical threats. The Russia/Ukraine conflict is one example, with several layers of new sanctions imposed during the past few months, some of which operate with unique limitations.

In the area of export controls, last year, convictions resulting from BIS investigations almost doubled from the prior year, and the amount of jail time imposed for export control offenses jumped by more than a factor of four. BIS's "end-use checks," which seek to ensure exports are not being used in violation of US controls, have risen steadily since 2008, and hit a 10-year high last year. Acting in tandem with OFAC, BIS has also recently implemented new export controls regulations relating to Russia.

Anti-money laundering oversight has also attracted increased attention from several US enforcers. Beyond the high-profile criminal enforcement actions in this space during the past few years, FinCEN is pursuing rulemaking to, among other things, augment customer due diligence obligations for financial institutions to identify and verify beneficial owners of customer accounts.

Against this background is the evolving compliance front of cyber-security. The Federal Trade Commission has brought several unfair trade practices actions alleging corporate failure to implement adequate security measures or to timely and fully disclose security breaches. The SEC has also pursued an enforcement action against company executives for failing to adequately safeguard data.

At bottom, compliance teams operate in a new normal—a global geopolitical environment with evolving compliance threats and demands. In this shifting landscape, corporate compliance programs must seek to continually adapt and respond. Periodic check-ups can be important, just as with any good health regimen. Compliance teams should seek to understand the full reach of potentially relevant enforcement agencies. Just to give a few examples of what are sometimes lesser-known corners of US enforcement policy: US export controls can apply not just to exports from the US abroad, but also to re-exports of goods from one foreign location to another; OFAC sanctions can apply, in some circumstances, not just to US entities, but also to non-US entities that "cause" US persons to violate OFAC sanctions; and BSA requirements can, in some instances, extend to finance-oriented subsidiaries of parent companies that would not ordinarily consider themselves financial institutions.

For any compliance system, it is advisable as well to monitor the latest enforcement developments. The recent sanctions on certain Russian persons and entities are a prime example. In quick succession, OFAC issued a series of new, and in some instances complex, sanctions followed by a series of answers to frequently asked questions clarifying certain aspects of the new embargoes. Constant monitoring of these developments can prove helpful, not just to effective compliance, but also to maximizing business opportunities.

In the context of a new joint venture, partnership, merger, or acquisition, compliance check-ups can also be warranted and new compliance protocols may, in some situations, be appropriate. Consideration may be given to a number of matters, including whether additional laws now apply to the controlling parent company and any pre-existing or new subsidiaries. These considerations can take on particular significance in transactions involving the combination of domestic and foreign business entities.

In the end, whether a compliance program is newly minted or decades old, it is always good to keep in mind why compliance programs exist in the first place. Given how active enforcement agencies are today, some have expressed the view that the most important reason to have a compliance program is to demonstrate good faith when a breakdown occurs, to mitigate the fallout from any wrongdoing when interacting with an enforcement agency. While this is certainly an important aspect of compliance, compliance programs exist, first and foremost, to seek to prevent misconduct from occurring in the first place. Constant tending of compliance policies can help avoid at least some of the broken windows and other damage that can occur in a global corporate household.

Author Biography

John D Buretta *is a partner in the Litigation Department of Cravath, Swaine & Moore LLP. His practice focuses on advising corporations, board members, and senior executives with respect to internal investigations, criminal defense, and regulatory compliance, including matters related to the FCPA, antitrust, fraud, insider trading, money laundering, OFAC, and export controls. Mr Buretta returned to Cravath in November 2013, following 11 years of service in the Department of Justice (DOJ), where he most recently held the position of Principal Deputy Assistant Attorney General and Chief of Staff, the number-two ranking official in the Criminal Division. While at the DOJ, Mr Buretta supervised the preparation of the DOJ and SEC's Resource Guide to the US Foreign Corrupt Practices Act, issued in November 2012, and was appointed Director of the Deepwater Horizon Task Force.*