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.” 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.

On the US sanctions front, OFAC continues rigorous enforcement of a spectrum of embargoes, trade sanctions, and Executive Orders. Since 2005, OFAC settlement amounts have more frequently reached into the hundreds of millions of dollars, with nearly $13 billion in penalties imposed during the past five years, including over $8 billion in penalties imposed so far this year. 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, violations 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 ramped steadily since 2008, and hit a 10-year high last year. Acting in tandem with OFAC, BIS has recently implemented new export controls regulations relating to Russia.

Anti-money laundering oversight has also attracted increased attention from 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. Whether a compliance program is newly minted or decades old, it must seek to continually adapt and re-scape, corporate compliance programs exist in the first place. 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.
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” cases. 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 focus has also included 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 swap dealers.

On the US sanctions front, OFAC continues aggressive enforcement of a spectrum of embargoes, sanctions, and related Executive Orders. Since 2003, OFAC settlement terms have frequently reached into the hundreds of millions of dollars, with nearly $3 billion in penalties imposed during the past year, including over $1.2 billion in penalties imposed so far this year. 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 violations 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 violations 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 enforcement agencies. 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 cybersecurity. The Federal Trade Commission has brought several unfair trade practice 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 companies 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. Ongoing 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 courses 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-related subsidiaries of parent companies that would not ordinarily consider themselves financial institutions.

For any compliance system, it is advisable to as well monitor the latest enforcement developments. The recent sanctions against 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 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, and to be in a position to interact 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 tend ing of compliance policies can help avoids 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. Mr. Buretta advises 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 2016, following a six-year assignment as Assistant Attorney General and Chief of Staff, the number-two ranking position in the Criminal Division. While at the DOJ, Mr. Buretta supervised the preparation of the DOJ’s Foreign Corrupt Practices Act Resource Guide to the US Foreign Corrupt Practices Act, issued in November 2014, and was a key member of the Director of the Deepwater Horizon Task Force.