Client Alert:

Impact of DOJ's 2020 Update: What Compliance Leaders Need to Know Now

Stephen Martin

Partner, StoneTurn
smartin@stoneturn.com
+1 303 747 6398

Jamen Tyler

Managing Director, StoneTurn
jtyler@stoneturn.com
+1 303 747 4005

Thomas Fox

Senior Adviser, StoneTurn
tfox@stoneturn.com
+1 713 547 4000

Just over a year since the U.S. Department of Justice (DOJ) published its last update, the DOJ's Criminal Division has again updated its guidance on "Evaluation of Corporate Compliance Programs." As with the 2017 and 2019 guidance documents, the 2020 Update lays out factors and questions federal prosecutors should consider when evaluating the effectiveness of a compliance program. While the 2020 Update retains most of the substance of the 2019 Update, it adds a number of key points that can help companies, compliance officers and counsel better understand DOJ expectations—and what companies and compliance professionals should do to meet them in maintaining an effective compliance program. Here, we highlight the key changes and discuss the areas of focus in the 2020 Update.

Risk Assessments and Continuous Monitoring/ Improvement Remain Key Priorities

Given the emphasis on risk assessments in the 2019 Update, it should come as no surprise that risk assessments once again take center stage in the 2020 Update. The 2019 Update stressed the importance of structuring, resourcing and continuously improving compliance programs based on effective risk assessments and "periodic review" of the company's risk profile. The 2020 Update further explains that companies can no longer rely on periodic risk assessments that capture only "a 'snapshot' in time" at their company Instead, corporate compliance programs will be assessed based "upon continuous access to operational data and information across functions." Prosecutors will further consider whether a company tracks and incorporates "lessons learned"

StoneTurn

from both "prior issues" and those of companies in the same industry and/or location into its risk assessment process. This theme is repeated in the "Continuous Improvement" section and framed as whether a company reviews and adjusts its compliance program based on both its own "misconduct" and misconduct of "companies facing similar risks."

ACTION ITEM:

Data Access and Ongoing Risk Assessment

Based on the 2020 Update, compliance professionals should ask themselves if they have access to continuous and real-time data about risks within their organization, industry and geographies. Are you able to monitor risks between siloes in your organization? Do you track issues identified between risk assessments and revise your compliance program (and assessment process) accordingly? Do you track enforcement actions or misconduct of your peer organizations? For many, if not most, companies, the answer to one or more of these questions is "no."

To remedy this gap, companies should begin by pulling and organizing compliance-related data, including accounting reviews, whistleblower reports, due diligence reports and compliance news bulletins, and continuously monitor for new or changing risks in their operations. Compliance professionals should also look beyond the risks facing their own organization to understand risks faced by similarly-situated companies. At a minimum, CCOs, compliance professionals and counsel will need to stay abreast of international anti-corruption enforcement actions within their industries and where their company may be doing business. If new risks are identified within a company's operations, industry or geography—even between formal risk assessments—both the compliance program and risk assessment process should be reviewed and, if appropriate, revised and enhanced.

M&A Changes: Post-Close Integration and Compliance Reviews

The clear emphasis of the 2020 Update with respect to compliance in the mergers and acquisition (M&A) space is the expectation of both pre-acquisition due diligence and "timely and orderly" post-close integration. While the revised guidance recognizes that pre-acquisition due diligence is not always possible, the additional language makes clear that the DOJ will expect an explanation if reasonable or appropriate due diligence is not completed.

A perhaps more significant change to the M&A section in the 2020 Update is the addition of several references to post-close integration and compliance reviews. These changes emphasize the importance of having a process in place to smoothly and promptly transition newly-acquired entities into a company's compliance program. They also reinforce the DOJ's focus on processes for post-close audits of "misconduct or misconduct risks" at the newly-acquired entity.

ACTION ITEM: Ensure Effective Due Diligence and Post-Close Compliance Reviews and Integration

Compliance professionals should work with their company's strategy or deal teams to make sure they are aware of and involved in potential M&A transactions as soon as possible after a potential target is identified. They should also consider creating a framework or checklist for compliance due diligence to help ensure consistency and completeness of pre-acquisition compliance reviews. If the compliance due diligence team is restricted from completing a fulsome due diligence review, compliance professionals and their counsel must carefully track and document the basis for those restrictions. They should also consider consulting the DOJ for guidance on how to proceed if a rule, regulation or other legal restriction prevents them from conducting appropriate pre-acquisition due diligence review.

After the deal closes, the DOJ will generally expect companies to conduct a comprehensive risk assessment on the newly acquired entity This is especially important if you were unable to conduct due diligence pre-close, but should generally be done for all entities within a year of their acquisition. Companies that have not been conducting post-close risk assessments on newly-acquired entities should, at minimum, ensure that any previously-acquired entities are reviewed as part of their ongoing risk assessment process and establish a process for conducing targeted risk assessments of newly acquired entities going forward.

Companies should also review their past performance with the integration of acquired entities. Are these entities fully integrated into your company's compliance program? If the answer is no, how long ago was the company acquired? Generally speaking, target entities should be integrated within around 18 months of acquisition. If your company has yet to integrate entities into your compliance program beyond that point, your compliance team should make sure they have either a plan for completing the integration process or a clear, documented explanation for why complete integration is unnecessary.

To help ensure efficient and effective post-close risk reviews and compliance integration, compliance professionals and their counsel can put a post-close framework in place

to guide post-close compliance decision-making and planning. This framework should include an overview of decisions that need to be made, stakeholders that need to be consulted, and other topics common to any integration process. It should also include a general overview of the post-close risk assessment process. While no two post-close integration/risk assessment processes will be the same, having a clear understanding of how to address them can help expedite both the planning and the implementation of your post-close compliance activities.

Third-Party Management: Beyond Due Diligence and Contract Provisions

Even in 2020, third parties still represent the highest risk under the FCPA. The 2020 Update reflects this exposure by shifting focus from a company's "third party due diligence practices" (as in the 2019 Update) to its overall "third party management practices." In addition to this revised language, the 2020 Update asks prosecutors to look at whether the company manages risks posed by third parties "throughout the lifespan of the relationship, or primarily during the onboarding process."

This revised language and additional question make clear that management of third parties is a process, not just a due diligence exercise that ends after the contract is executed. While both due diligence and contractual compliance obligations remain important, the 2020 Update re-emphasizes that managing compliance risks posed by each third-party relationship must extend beyond onboarding.

ACTION ITEM:

Continuous Third-Party Oversight

Compliance professionals should continuously monitor compliance risks posed by each third party and, if necessary, adjust the relationship (including payment terms, oversight, and scope of work) to address those risks. An effective compliance program will include processes and procedures for doing so, including a third-party management program that oversees the entire lifecycle, from due diligence to onboarding to ongoing review and contract renewal or completion. In light of the 2020 Update, compliance professionals should conduct a review of their existing third-party program to determine whether it meets DOJ expectations.

Are Compliance Resources Adequate and Empowered?

The 2020 Update provides further clarification about what differentiates an effective program from a mere "paper program," particularly with respect to resourcing and authority of the Chief Compliance Officer and other compliance personnel. The revisions call out the need for programs to be adequately "resourced" and "empowered" and reiterate that those with day-to-day compliance responsibility need to have adequate resources, authority and access to the company's "governing authority." The update also adds a question for prosecutors to consider whether a company "invest[s] in further training and development of the compliance and other control personnel."

ACTION ITEM:

Professional Development and Board Access

The 2020 Update makes clear that there must be ongoing professional development for the CCO, compliance team members and the other control personnel in the company. "Other control personnel" is not defined in the guidance, but appears to include personnel in legal, supply chain/procurement, human resources, accounting/finance or internal audit or other functions that make decisions regarding compliance issues. In addition to regular training on evolving compliance best practices, a clear path for career and professional development should be established. In addition, the compliance team should have direct access to the Board or alternate company oversight.

Data, Data, Data: Is it Readily Available?

A completely new line of questioning in the 2020 Update focuses on "Data Resources and Access" by the compliance and control personnel. Specifically, the new questions ask whether these personnel have "sufficient" access, direct or indirect, to relevant data to allow for timely (and, implicitly, ongoing) monitoring of the compliance program. These questions indicate that the DOJ expects a company to work to make compliance-related data readily available to the CCO and compliance function and to remedy any "impediments…that limit access to relevant sources of data."

ACTION ITEM:
Create Custom Compliance Dashboards and/or KPIs

The 2020 Update includes a much more stringent requirement than the CCO calling up IT to find out what data might be available to monitor on an ongoing basis. Every company must take affirmative steps to make holistic data available and get to it the compliance team in some type of usable format. This type of digitally enabled compliance can be achieved in many forms, and third-party advisers and/or software providers can help companies establish custom compliance dashboards or key performance indicators (KPIs) as a starting point.

Ensure Consistency Around Institutional Justice and Fairness

The 2020 Update reiterates the need to not only apply disciplinary actions and incentives consistently, but also to "monitor… investigations and resulting discipline to ensure consistency." This mandate speaks to institutional justice and institutional fairness which, ultimately, are cornerstones of any effective compliance program. If a company turns a blind eye to wrong-doing by the highest grossing salesperson due to his or her perceived value to the company, employees may conclude that there are no consequences to misconduct or worse, that the only way to get ahead in an organization is to lie, cheat and steal.

ACTION ITEM:
Senior Leadership Commitment

Top management must demonstrate that it does not actively or tacitly encourage illicit behavior with ample documentation of investigation outcomes and disciplinary measures. The compliance function must be empowered to conduct investigations, discipline as needed and provide incentives as appropriate. Just as importantly, the compliance team must also have resources to both confirm that these activities are conducted consistently throughout the organization and address and remediate processes that allow for disparate treatment, if identified.

Conclusion

While at first glance the changes in the 2020 Update may see small, their implications are far-reaching. Indeed, the publication itself indicates that the DOJ remains focused on both enforcement and the need for effective corporate compliance programs despite the current COVID-19 related economic downturn and operational restrictions. This means that companies should avoid the temptation to put off risk assessments or program reviews and enhancements. Instead, compliance professionals and their counsel should review the update carefully and pay particular attention to changes that may underscore gaps in their existing compliance programs. They should also consider conducting a full review of their company's compliance programs or, at minimum action areas highlighted by the 2020 Update, for potential gaps and opportunities for enhancement.