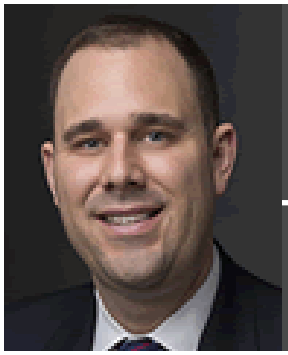


PANEL DISCUSSION: CONDUCTING INTERNAL INVESTIGATIONS - BEST PRACTICES AND CURRENT TRENDS

James Melendres
Snell & Wilmer (Phoenix, AZ)
602.382.6555 | jmelendres@swlaw.com

Internal Investigations: The Impact of DOJ's Recently Announced Compliance Program Evaluation Guidance
James Melendres, Brett Johnson and Aloke Chakravarty

Recent Department of Justice ("DOJ") guidance regarding its evaluation of corporate compliance programs has important implications for the conduct of internal investigations. In particular, in April 2019, DOJ issued updated guidance to DOJ prosecutors on how to assess corporate compliance programs when conducting an investigation, in making charging decisions and in negotiating resolutions. Understanding this updated guidance, entitled "Evaluation of Corporate Compliance Programs," is essential for implementing an effective compliance program and conducting internal investigations as part of such program.

This article will discuss DOJ recent corporate compliance program evaluation guidance, the practical consequences for internal investigations, and factors senior executives and in-house counsel may want to consider before and during an investigation based on DOJ's renewed focus on internal compliance controls.

Evaluation of Corporate Compliance Programs: DOJ's Updated Guidance

The updated guidance poses three basic questions for the evaluation of a compliance program: Is the program well designed? Is the program being implemented effectively? Does the program work in practice? These basic elements have long been considered by DOJ and the courts. For example, the Justice Manual states that the adequacy and effectiveness of the corporation's compliance program is one of the factors to be considered in making a charging decision, and it may be one of the most significant influencers to avoid punitive decisions. And U.S. Sentencing Guidelines Section 8C2.5(f) provides that an effective compliance program significantly reduces a corporate entity's culpability score, potentially reducing a fine by millions of dollars.

DOJ's guidance answers these three core questions and provides a template for compliance. Specifically, compliance programs will be measured first by how thoughtfully a company designs:

- Risk assessment processes
- Adequate policies and procedures
- Training and communications
- Confidential reporting and investigations conduits
- Third-party relationship management
- Due diligence for merger activity

Implementation will be measured by the:

- Commitment of management
- Autonomy and adequate resourcing of compliance
- Appropriate incentives and discipline

Whether a compliance system actually works will be measured by its:

- Improvement, testing and feedback systems
- Investigations of misconduct
- Analysis and response to misconduct

Several of the components described above have a direct bearing on the triggers for, and conduct of internal

investigations.

Effective design empowers the right people to make policies work on the ground, not just on paper. An effective compliance program empowers corporate actors to take remedial action without over-inclusively flooding a reporting system with noise. Companies should ask "where do the problems occur and who should be empowered to stop them?" In the areas of heightened risk, reporting protocols are expected to be more robust—police officers are expected to focus their resources on high-crime areas. Effective design can thus be both economical and minimally invasive to regular operations. Conversely, relying on stringent controls in a low-risk area provides little counterweight to significant failures in a high-risk one.

Design should consider the importance of tailoring palatable conduits for reporting. The corollary to empowering those close to the action is the difficulty in identifying errors of people you know. The updated guidance emphasizes that "an efficient and trusted mechanism by which employees can anonymously or confidentially report" misconduct is a "hallmark of a well-designed compliance program" and "highly probative" of an effective program. The updated guidance places a greater emphasis on culture and easy, anonymous reporting. One way to overcome human nature is to routinize, anonymize and normalize the process. This is why algorithmic compliance measures have made compliance efforts so much more effective to overcome the natural human hesitance to report misconduct or the "fear of retaliation." An effective compliance program must make it easy for people at all levels to do the right thing.

To implement a program effectively, you must learn from mistakes. The updated guidance emphasizes that past violations and the company's reaction to them is critical. Virtually every company will face the specter of some kind of regulatory violation given enough time. The guidance acknowledges this reality and does not equate every offense as a proxy for a deficient compliance program. Acknowledging the inevitability of wrongdoing means that an effective compliance program must also have a robust protocol for self-reporting.

Self-reporting is a sensitive task, but a thorough internal investigation followed by prompt and full disclosure can reap large rewards. For example, the Foreign Corrupt Practice Act Corporate Enforcement Policy states that prosecutors place "a high premium on self-reporting, along with cooperation and remedial efforts, in determining the appropriate resolution of FCPA matters." In particular, when a company cooperates and remediates, and also voluntarily self-discloses misconduct, it is eligible for a full range of potential mitigation credit. The DOJ provided guidance criteria for a company to qualify for credit in three different categories: (a) voluntary self-disclosure; (b) cooperation; and (c) remediation.[1]

More specifically, to receive credit for self-reporting, a company must make the disclosure within a reasonably prompt time after becoming aware of the offense and before there is a threat of disclosure by someone else or a government investigation relating to the conduct.

To qualify for cooperation credit the DOJ has set forth a number of requirements that must be met. For example, some of the prerequisites include: (a) "disclosure on a timely basis of all facts relevant to the wrongdoing at issue;" (b) "[p]roactive cooperation, rather than reactive; that is, the company must disclose facts that are relevant to the investigation, even when not specifically asked to do so;" (c) "[p]reservation, collection, and disclosure of relevant documents and information relating to their provenance;" (d) "where requested, de-confliction of witness interviews and other investigative steps that a company intends to take as part of its internal investigation with steps that [DOJ] intends to take as part of its investigation;" and (e) "where requested, making available for interviews by the Department those company officers and employees who possess relevant information."

A company seeking leniency under the FCPA Corporate Enforcement Program must also undertake appropriate remediation consistent with DOJ guidelines.

Moreover, at the ABA's March 2018 White Collar Conference, DOJ expanded its corporate leniency program beyond FCPA violations. In particular, DOJ officials announced that they will use the FCPA Corporate Enforcement Policy as nonbinding guidance in other criminal cases. In particular, John Cronan, the acting head of DOJ's Criminal Division stated, "We intend to embrace, where appropriate, a similar approach and similar principles — rewarding voluntary self-disclosure, full cooperation, timely and appropriate remediation — in other contexts."

Consistent with DOJ's corporate leniency policy, the updated guidance regarding DOJ's evaluation of compliance programs states, "[I]f a compliance program did effectively identify misconduct, including allowing for timely remediation and self-reporting, a prosecutor should view the occurrence as a strong indicator that the compliance program was working effectively."

1 U.S. Attorney's Manual, § 9-47.120 – FCPA Corporate Enforcement Policy, available at https://www.justice.gov/criminal-fraud/file/838416/download

Proactively examining a business' vulnerabilities and investigating and reporting errors when they do occur is consistent with upholding a culture of compliance, but also helps negate intent, and allows companies to craft their own investigations instead of conceding to the government.

Proving the negative is often worth the effort. While prosecutors may be cynical, data helps make cases. In monitoring a program's efficacy, steps that show positive feedback complement those that show when errors occur. The guidance asks prosecutors to consider whether the program has "collected, tracked, analyzed, and used information from its reporting mechanism." An effective compliance program will flag many instances where there is no wrongdoing but shows that a conscientious observer felt comfortable reporting a possible issue. A company's reaction to the absence of a violation can demonstrate sincerity just as a reaction to actual wrongdoing might. Citing examples where a company undertook a thorough and well-documented investigation and concluded there was no wrongdoing is preferable to the alternative. Determining where false positives occur can also aid in the fine tuning of a program's design and could save time and money by implementing tweaks that will avoid such results.

What this Means for Corporate Executives and In-House Counsel

Senior executives and in-house counsel may want to prepare now for future investigations based on how government attorneys will evaluate their company's compliance program pursuant to the April guidance.

The DOJ's updated guidance is helpful and more detailed than its prior iteration, but it is complementary to other sources as well, such as the Benczkowski Memorandum from October 2018. Ultimately, the focus in the updated guidance is on results; whether the program is actually effective. There is no magic number of resources to allocate to compliance, and efforts that emphasize uncontextualized spending or top-level inputs will not be as persuasive as those that show that a company has thought through its operations and compliance risks, and that it has taken proactive steps to maintain an effective and adapting program. It bears reminding that one of the principle goals of prosecutors is to deter wrongdoing—by a specific company, but also by other companies generally. The guidance emphasizes that effective compliance requires preparation, vigilant oversight, commitment of culture and resources, and adaptability to changing landscapes. The updated guidance can be an effective tool to secure buy-in from operational executives for implementing measures that may help weather the inevitable storms ahead.

Snell & Wilmer

Conducting Internal Investigations: Best Practices and Current Trends

© 2019 Snell & Wilmer

Panelists

James Melendres, Moderator
Snell & Wilmer
Chair, White Collar Defense and Investigations

Brett Johnson
Snell & Wilmer

Additional Panelist(s) TBD

© 2019 Snell & Wilmer

DOJ Evaluation of Corporate Compliance Programs: April 2019

- The updated guidance poses three basic questions for the evaluation of a compliance program:
  - Is the program well designed?
    - Confidential reporting and investigations conduits
  - Is the program being implemented effectively?
  - Does the program work in practice?
    - Investigations of misconduct
    - Analysis and response to misconduct
    - Self-reporting

© 2019 Snell & Wilmer

FCPA Corporate Enforcement Policy

- Full range of mitigation credit based on following criteria:
  - Voluntary self-disclosure
  - Cooperation*
  - Remediation
- Presumption of declination (assuming absence of a non-exclusive list of "aggravating factors")

© 2019 Snell & Wilmer

FCPA Corporate Enforcement Policy

- Cooperation*
  - Disclosure on a timely basis of all relevant facts
  - Proactive cooperation, rather than reactive
  - Preservation, collection, and disclosure of relevant documents and information relating to their provenance
  - De-confliction of witness interviews and other investigative steps
  - Officer and employee interviews

© 2019 Snell & Wilmer

FCPA Corporate Enforcement Policy

- Expansion announced by DOJ at March 2018 ABA White Collar Conference
- Nonbinding guidance in other criminal cases
- John Cronan, the acting head of DOJ's Criminal Division stated, "We intend to embrace, where appropriate, a similar approach and similar principles — rewarding voluntary self-disclosure, full cooperation, timely and appropriate remediation — in other contexts."

© 2019 Snell & Wilmer

What Prompts an Investigation?

- Whistleblower / Hotline complaint
- An inquiry or investigation by a governmental agency, such as DOJ, a State Attorney General or the Securities and Exchange Commission
- Notice from outside auditors
- News articles
- A shareholder lawsuit or demand

© 2019 Snell & Wilmer

Investigative Process

- Document preservation
- Preliminary "document interviews"
- Document collection
- Document review
- Witness interviews
- Conclusions

© 2019 Snell & Wilmer

Witness Interviews

- **"Corporate Miranda"/Upjohn disclosure**
  - Counsel is representing the company or board
  - The attorney does not represent the employee personally
  - Although the conversation is protected by the attorney-client privilege, the company may choose to disclose information to third parties

© 2019 Snell & Wilmer

Conclusions

- Prepare findings
- Share conclusions with client
- Form of report
  - Written report or outline
  - Oral presentation
  - Combination of oral and written report

© 2019 Snell & Wilmer

Conclusions

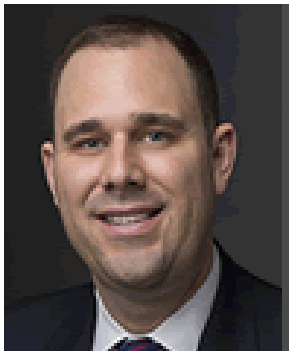
- Presentation to any other appropriate audiences
  - –Auditors
  - –Regulators
  - –Shareholders
- Be cautious about privileged information

© 2019 Snell & Wilmer

Questions?

©2019 All rights reserved. Notice: As part of our effort to inform you of changes in the law, Snell & Wilmer provides legal updates and presentations regarding general legal issues. Please be aware that these presentations are provided as a courtesy and will not establish or reestablish an attorney-client relationship or assumption of responsibility by Snell & Wilmer to take any action with respect to your legal matters. The purpose of the presentations is to provide seminar attendees general information about recent changes in the law that may impact their business. The presentations should not be considered legal advice or opinion because their individual contents may not apply to the specific facts of a particular case.

© 2019 Snell & Wilmer



JAMES P. MELENDRES

Partner

SNELL & WILMER (Phoenix, AZ)

602.382.6555 | jmelendres@swlaw.com

James Melendres co-chairs the Investigations, Government Enforcement and White Collar Protection practice and the Cybersecurity, Data Protection and Privacy practice. He regularly conducts internal investigations and represents companies in a wide variety of matters relating to federal and state criminal, civil and regulatory enforcement. James also advises companies regarding the full life cycle of enterprise risks associated with cybersecurity, including before, during and after a data breach or other cyber-attack.

James further assists clients in developing and implementing crisis management and public relations strategies. He has appeared on CBS, CNBC and MSNBC and been quoted in The Wall Street Journal and Bloomberg, among other publications.

Prior to joining Snell & Wilmer, James served as a federal prosecutor and led high-profile and complex matters, including the prosecutions of former Central Intelligence Agency Director David Petraeus and the leader of the Tijuana Cartel. He also served in the leadership offices at the Department of Justice in Washington, D.C., and in his role as counsel to the Assistant Attorney General for National Security, James helped manage the DOJ National Security Division and counseled senior DOJ officials on a wide variety of matters - from high-profile cyber investigations and related litigation to the strategic use of trade sanctions to counter cyber-related national security threats.

Related Services

- Cybersecurity, Data Protection and Privacy
- Investigations, Government Enforcement and White Collar Protection

Representive Experience

- Conducted internal investigation for university in connection with Department of Justice “Varsity Blues” college admissions prosecution
- Conducted internal investigation and defended company in parallel investigations by Inter-American Development Bank and Department of Justice Foreign Corrupt Practices Act Unit
- Conducted internal investigation for company regarding civil and criminal False Claim Act allegations
- Defended company in investigation by Securities and Exchange Commission regarding fraud allegations
- Represented public company in prosecution by U.S. Attorney’s Office for the Southern District of New York regarding indictment charging individuals with fraud and kickback scheme
- Represented public company in prosecution by U.S. Attorney’s Office for the Middle District of Florida regarding indictment charging individual with obstruction of justice and material support for terrorism
- Represented non-profit organization in prosecution by Department of Justice Fraud Section regarding indictment charging individuals with fraud, money laundering, and false statements
- Represented venture capital firm in investigation by Securities and Exchange Commission regarding material misstatement allegations

Professional Recognition and Awards

- The Best Lawyers in America®, Criminal Defense: White Collar (2019-2020)

Education

- Stanford Law School (J.D., 2003)
- Dartmouth College (A.B., cum laude, with high honors, 2000)