PROGRAM MATERIALS
Program #30164
July 8, 2020

Flexibility and Vigilance: Effectively Manage Government and Internal Investigations During COVID-19

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

Buchanan Ingersoll & Rooney PC

Flexibility and Vigilance: Effectively Manage Government and Internal Investigations During COVID-19

John P. Cunningham, Shareholder
Jason R. Parish, Shareholder
Martin J. Amundson, Associate

July 8, 2020

Agenda

- Investigative agency responses to COVID-19
- Strategies for conducting remote / hybrid internal and government investigations
  - Privilege considerations
  - Document collection and review
  - Interviews
  - Reporting
  - Investigation resolution
- Best practices for conducting investigations amidst COVID-19
- Additional published COVID-19 era investigation resources

Investigative Agency Responses to COVID-19

Federal and State Agency Responses

- U.S. Department of Justice
- Federal Trade Commission
- Securities and Exchange Commission
- Office of Foreign Assets Control
- Office of the Special Inspector General for Pandemic Recovery
- U.S. Department of Homeland Security / U.S. Customs and Border Protection
- State Attorneys General

U.S. Department of Justice

- Response timeline:
  - March 16: AG directs USAOs to prioritize investigation and prosecution of COVID-19 related crimes
  - March 18: DAG instructs USAOs and “supporting components” to remain active and committed to protecting the public and sustaining all categories of federal investigations
  - March 20: First enforcement action filed against website allegedly offering vaccine kits in exchange for shipping fee
  - March 24: AG announces creation of national task force to address COVID-19 related hoarding and price gouging of critical supplies
  - March 24: DAG directs the DOJ to pursue COVID-19 related crimes under longstanding criminal and antitrust statutes

Federal Trade Commission

- Response timeline:
  - March 9: FTC / FDA send first warning letters regarding unsupported claims that products treat or prevent COVID-19
  - March 24: DOJ / FTC announce antitrust guidance and expedited procedures for business collaborations to address COVID-19
  - April 13: DOJ / FTC issue statement regarding no-poach and wage-fixing agreements for critical workers

Securities and Exchange Commission

- Actively monitoring markets for frauds, illicit schemes, and other misconduct related to COVID-19
- Commenced several enforcement actions against issuers and individuals alleging COVID-related fraud, including:
  - SEC v. Gomes, *et al.* (6.9.20) – alleged fraudulent scheme that generated more than $25 million from illegal sales of microcap companies' stock, including four companies that were the subject of recent SEC trading suspension orders
  - SEC v. Applied Bioscience (5.14.20) – company charged with alleged false claims related to the offering and shipping of finger prick COVID tests
  - SEC v. Praxsyn Corporation *et al.* (4.28.20) – company and CEO charged with false claims that the company was able to supply large quantities of N95 or similar masks

Other Federal and State Agencies

- Office of Foreign Assets Control
  - Encourages persons, including financial institutions and other businesses affected by the COVID-19 pandemic, to contact OFAC as soon as practicable if it may experience delays in meeting deadlines associated with regulatory requirements administered by OFAC, such as:
    - (1) blocking and reject reports, (2) responses to administrative subpoenas, (3) reports required by general or specific licenses, and (4) any other required reports or submissions
- Department of Homeland Security, U.S. Customs and Border Protection
  - Monitoring imports and exports that may contain counterfeit or illicit goods
  - Confiscating prohibited medical supplies, including fraudulent N95 masks

Looking Ahead

- Government investigations are continuing – however:
  - Many government attorneys (and clients) continue to work from home with travel restrictions
  - Continued court disruptions
  - Practical difficulties impact client responses
- What this means:
  - Slower pace for ongoing investigations
  - Some de-prioritization of less significant / non-COVID-19 related investigations
  - Increased use of tolling agreements
  - Increased reliance on videoconferencing and other technology

Strategies for Conducting Remote / Hybrid Internal and Government Investigations

Attorney-Client Privilege and Work Product

- Attorney-client privilege is generally waived if a third-party is present during the communication
- Telephone and video interviews make it difficult to control who is present during (or listening to) an interview
- To avoid a potential waiver, counsel should explain at the outset of the interview the importance of confidentiality and give clear instructions about the potential consequences of having a third-party present during the interview
- To ensure maximum security, use one of the many secure and encrypted audio/video software options
- Smart speakers and digital personal assistants should also be disabled during interviews

Document Collection and Review

- Though many states are beginning to reopen, many businesses remain voluntarily closed or are having their employees work remotely for the foreseeable future
- Not having employees together in a single location (or in their typical office spaces) can slow and / or frustrate the physical collection of documents
- And as many companies have been forced to lay off or furlough employees, data and document custodians may not be readily available to answer questions that arise during the collection process

Document Collection and Review (cont'd)

- The risk of a second wave of COVID-19 infections in the fall could lead to renewed lockdowns or stay-at-home orders
- It is critical that companies take steps now to mitigate the effects of such orders
- Companies should be organized and conduct custodian interviews at the outset of an investigation to determine where relevant information is stored or maintained
- Obtain passwords and other materials necessary for accessing files at the beginning of the investigation
- Communicate openly and regularly with the information technology department to get directory maps for available electronic databases

Interviews

- Remote investigations may require that witness interviews be conducted telephonically or by video conference
- Because the interview will not be held face-to-face, both the witness or the interviewer may be tempted to record the interview
- Companies conducting virtual interviews should be aware of state and federal laws relating to recordings
- It is also possible that the interviewer and interviewee could be in different jurisdictions with differing rules
- Recording a conversation without obtaining proper consent (if required) could result in civil and/or criminal penalties

Interviews (cont'd)

- Regardless of the jurisdiction, an interviewer should notify the interviewee at the outset whether the interview will be recorded
- The interviewer should also ask the interviewee if he/she is recording the interview
- Even if the interviewee denies that they are recording, the interviewer should nonetheless state that the company does not consent to recording
- Recordings can also lead to discovery and privilege issues
- While written notes are often viewed as attorney work product, recordings may not be entitled to the same protections and could therefore be discoverable in litigation

Interviews (cont'd)

- It is vital for companies to ensure that appropriate security is in place to protect the integrity of a virtual interview
- As the use of various virtual platforms has increased during the past several months, so have instances of third parties intentionally or inadvertently gaining access to conference lines or video meetings
- Any conference line or video should be password protected and/or encrypted as circumstances require to preserve the requisite security

Reporting

- As companies and government agencies continue to operate remotely, companies conducting internal or government-initiated investigations may need to report findings via telephone or video conference
- As with witness interviews, attendees of these meetings should also be reminded of the importance of privilege, work product, and confidentiality
- If appropriate, attendees should be provided with instructions about notetaking and/or dissemination of information to outside individuals
- Any materials provided to attendees should be conspicuously marked as "Privileged and Confidential," as necessary and appropriate

Investigation Resolution

- Many companies will struggle (even more so than normally) with whether to disclose potential wrongdoing to the government (and ultimately agree to a penalty or fine) when their financial health is increasingly uncertain
- Companies concerned about their ability to pay a fine or penalty because of their financial health should proactively raise the issue with investigators or prosecutors
- Open communication about COVID-19's impact on a company's finances will help both parties facilitate a fair and reasonable resolution
- Failure to proactively disclose this information could cause an investigator or prosecutor to operate under a mistaken assumption about a company's financial health, which could lead to otherwise-avoidable issues later in the investigation

Best Practices for Conducting Investigations Amidst COVID-19

Best Practices Checklist

1. Develop, maintain, and regularly update your internal investigation policy and associated procedures and protocols
2. Craft a thoughtful and comprehensive investigation plan at the outset of the inquiry with a tailored scope, realistic timelines, and consideration of the crisis
3. Maintain attorney-client privilege and work product protections by employing the secure and encrypted technology necessary to carry out investigative steps
4. Contemplate availability of resources to customize an investigation, particularly as those resources may be depleted during COVID-19
5. Conduct document collection and interviews in a manner that accounts for travel restrictions, remote work, and safety requirements for in-person interactions

Best Practices Checklist (cont'd)

6. In a government investigation, maintain consistent communication with investigators and/or regulators
7. Proactively alert investigators of developments related to COVID-19 that could impede or hinder the ability to meet deadlines or possible financial obligations
8. Update internal leadership and the board regularly, highlighting how the outcome may affect company resources and finances amidst the pandemic
9. Do not assume that, due to the pandemic, you can put "pencils down"; the government expects functioning entities to continue to investigate possible illegalities, irrespective of COVID-19 – albeit with potentially-relaxed timelines
10. These are difficult times and investigations, even without an ongoing pandemic, are extremely daunting; involve outside counsel in the process

Additional Published COVID-19 Era Investigation Resources

Additional Resources

https://www.law.com/corpcounsel/2020/05/11/how-to-effectively-manage-government-and-internal-investigations-during-covid-19/

Additional Resources

https://www.law360.com/articles/1282751/doj-guidance-provides-meaningful-compliance-road-map

Additional Resources

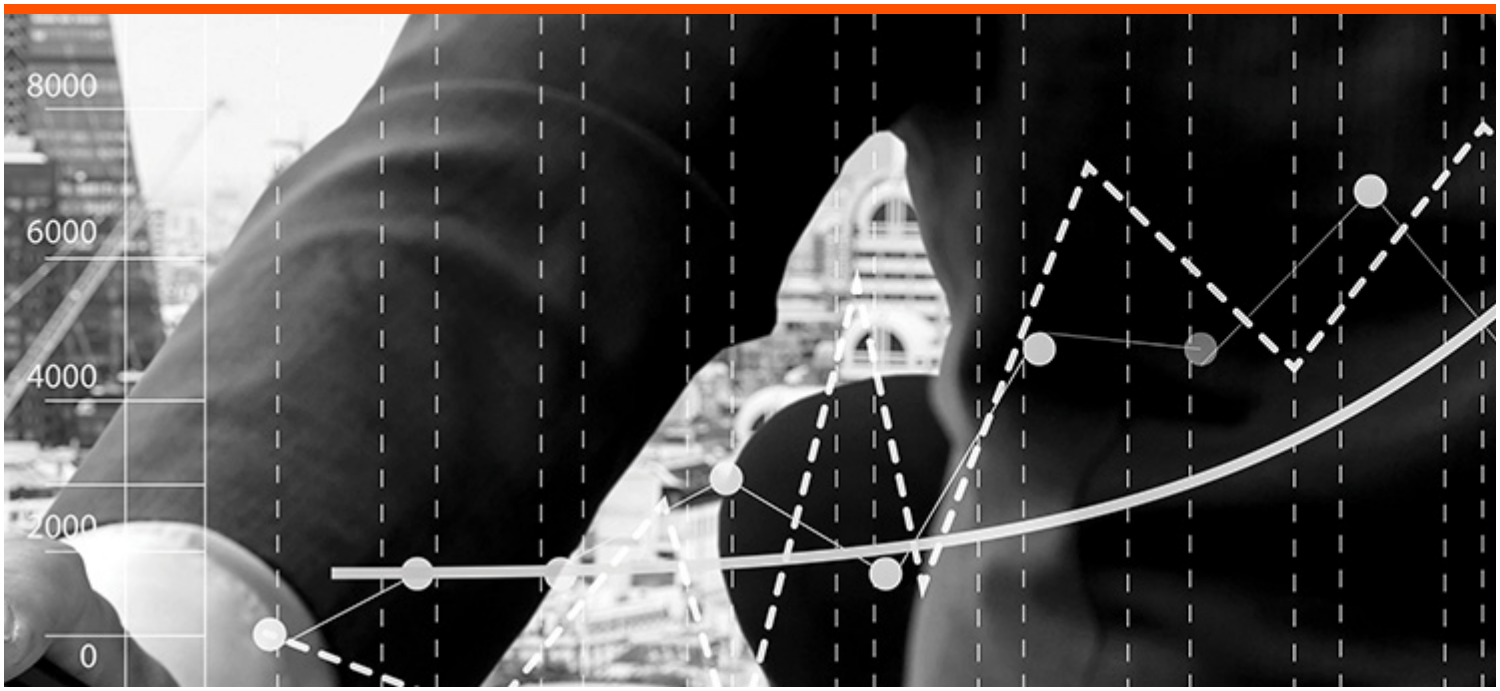
https://www.law360.com/articles/1270094/cos-must-prep-for-potential-federal-price-gouging-regs

Additional Resources

https://www.law360.com/articles/1252142/states-may-vigilantly-police-price-gouging-during-covid-19

Questions? Thank you!

- John P. Cunningham: john.cunningham@bipc.com
- Jason R. Parish: jason.parish@bipc.com
- Martin J. Amundson: martin.amundson@bipc.com



Buchanan Experience

Buchanan
Ingersoll·Rooney

https://www.bipc.com/

Price Gouging Should Not Be Another Symptom of the Coronavirus Outbreak

MAR 11 2020

As the COVID-19 infection rates grow across the United States, several states have all declared states of emergency in the past two weeks and the likelihood of more states following, or President Trump declaring a national state of emergency, also rises. So too does the possibility of product shortages – either from supply chain disruptions or unexpected increases in demand – which raises price gouging concerns.

Price gouging refers to the practice of raising prices to exploitive and unfair levels on goods and services that are in high demand and limited in quantity during natural disasters or other crises. In general, the government does not involve itself in business transactions, especially pricing. However, where there is a "temporary imbalance in bargaining power by virtue of an abnormal level of demand, in terms of both the number of consumers who desire the item and the sense of urgency that increases that desire," the government may intervene.[1] Most states have codified the circumstances under which pricing will be monitored through price gouging statutes. Consistent with a hands-off approach to government intervention in pricing, many pricing gouging statutes are limited in time and in scope. Even in the absence of a price gouging statute, states will look to intervene to ensure that consumers are not paying inflated prices during a crisis, as is the case of California and Washington where their Attorneys General have stated that they intend to combat any price gouging in their respective states:

> California Attorney General Xavier Becerra released a public statement indicating, "Californians shouldn't have to worry about being cheated while dealing with the effects of coronavirus. Our state's price gouging law protects people impacted by an emergency from illegal price gouging on medical supplies, food, gas, and other essential supplies."
>
> Washington State Attorney General Bob Ferguson similarly stated, "My office is investigating price gouging in the wake of the COVID-19 public health emergency. We do not identify the targets of our investigations, but we are taking formal investigative actions."

Other states will likely follow suit.

Price Gouging Statutes

There is no national price gouging regulation, although such regulation was considered in the wake of Hurricane Katrina. More than half of the states have some form of a price gouging statute.[2] While there are some consistent elements to the price gouging statutes, these statutes vary across states. For example,

California's price gouging statute makes violations a criminal offense. In contrast, Pennsylvania's statute is civil in nature, subjecting violators to penalties of up to $10,000 per violation as well as authorizing the imposition of injunctive relief and restitution. Pricing decisions therefore require a state-by-state analysis.

When Price Gouging Regulations Are Triggered

The majority of state price gouging statutes are triggered by a declaration of emergency from a city or county executive, a governor or the President of the United States. In California and Kansas, once a state of emergency has been declared the statute applies for 30 days and can thereafter be renewed. In North Carolina, the statute applies for 45 days. In Florida, it applies for 60 days. Some states like New York and Maine do not require a declaration of emergency, but rather are triggered by "an abnormal disruption" that recognizes events (man-made, natural and market forces) without a declaration of emergency. But statutory time frames can be easily overridden, and often are, as in the case of California, which has extended the 30 day period to September 4, 2020.

When a Price Increase Qualifies as a Price Gouge

There is no uniform threshold used to determine whether a price increase has become a price gouge. California has determined that an increase over 10 percent during a state of emergency is price gouging.[3] Other states, including Florida, are less clear, using phrases like "unconscionable"[4] and "excessive." At least two other states, including Georgia and Mississippi, simply say that any increases made after a declaration constitute price gouging. In states that have not set forth a threshold amount, whether or not an increase is a violation under the statute, becomes an issue to be determined in litigation. The variations that exist make it difficult for businesses increasing prices nationwide to steer clear of price gouging violations.

The calculation of an increase also varies by state. California's 10 percent is calculated based on what was being charged "by that person for those goods or services immediately prior to the proclamation or declaration of emergency."[5] Other statutes look at pricing in a period of time prior to the emergency.[6] The absence of uniformity in how price increases are calculated likewise makes compliance with price gouging statutes difficult.

What Goods and Services Are Impacted by Price Gouging Statutes?

Many price gouging statutes are limited to goods and services deemed necessary for consumer's health and welfare like fuel, food, batteries, medicine and housing.[7] But not all states are so limited. For instance, Arkansas, California, North Carolina and West Virginia, price gouging statutes apply to almost any good or service.[8] Most of the price gouging statutes are drafted to permit the emergency to dictate the scope of the law.

Price Gouging Enforcement in the Absence of a Statute

Simply because a state does not have a price gouging statute does not mean that a price gouging enforcement will not occur. The Attorney General for Washington, which like several other states does not have a price gouging statute,[9] has declared that he will tackle the issue:

We have something called the Consumer Protection Act which says you can't engage in an unfair business practice. It's our view, when there's a public health crisis[,] it's an unfair business practice to jack up your prices 20-30 percent on a common item, which makes it essentially unaffordable for so many who need to it literally save their lives.

While it is unclear whether the Washington courts will be receptive to the Attorney General Ferguson's legal position, businesses should expect State Attorneys General to monitor the marketplace and take corrective action. In short, the absence of a price gouging statute does not insulate a business from a state enforcement action.

Price Gouging Exceptions

Not all price increases, however, constitute price gouging. A price increase may be justified where the cost of doing business has increased. For example, in California where a "seller can prove that the increased price is directly attributable to increases in the cost of labor or materials needed to provide the good or service, the seller may not be liable under the statute." Similar cost and labor exceptions are recognized in most price gouging statutes.[10] It is likely that the coronavirus will have significant impacts on labor costs stemming from employee absence and compliance with health and safety laws.

Another avenue to avoid liability under a price gouging statute is to seek advance approval from the state for a price increase. For example, the Florida statute provides that a "price increase approved by an appropriate government agency" will not violate the price gouging statute.[11]

Considerations When Raising Prices During the Coronavirus Outbreak

Businesses should expect that State Attorney Generals will be actively monitoring pricing to ensure that consumers are not being harmed during the coronavirus outbreak. The impact of the coronavirus is global; in a few short months, it has already had significant impacts to distribution chains. And consumers are already creating shortages. Due to disruptions in the supply chain, businesses may need to consider raising prices.

Before increasing prices, businesses should consider the following:

Don't Assume That Price Gouging Statutes Don't Apply to You

Businesses should not assume that their product or service is exempted even in the face of statements that their product or service is not necessary to the health and well-being of consumers. For example, New

York's Attorney General webpage regarding price gouging has the following disclaimer:

> Note on the Coronavirus: Some consumers have complained to the Attorney General about recent increases in the price of surgical masks and respirators. However, the Surgeon General has stated that these items are not effective in preventing consumers from contracting the virus and has in fact have urged consumers to stop buying masks to ensure that there is no shortage for health care providers.

Despite indicating that medical masks are not necessary for the health and safety of residents, New York is treating medical mask price increases as a price gouge. Recent price increases to medical masks and sanitizing gel have triggered price gouging concerns. We are only in the early weeks of the outbreak, and as circumstances change, it is not out of the realm that products and services, not currently considered vital, may well become so.

Raising Prices Can Have Long-Term Consequences

If you are going to raise prices, be sure to consider the impact to your reputation and customer goodwill. Being accused of price gouging during a state of emergency can have long-term financial consequences. Many companies are experiencing this first-hand: Amazon has removed tens of thousands of items that are unreasonably priced. Using the price gouging statutes that specify a threshold as a guide, any pure profit increase at or above 10 percent may expose you to risk of price gouging.

Don't Surprise Customers with a Price at Checkout

State regulators rely heavily on consumer reporting in identifying businesses that are engaged in price gouging. If you are going to raise your pricing, be transparent about the increase. Make it clear to customers and vendors that the price increase reflects increased costs.

Be Prepared

If a price increase is required, a business should document with particularity any actual or anticipated cost increases or shortages, including when they occurred. Contemporaneous documentation is key to not only defending a price increase, but also in communicating with customers.

Maintain Antitrust Policies

Do not talk with your competitors. Antitrust laws still apply. And certain companies like those selling health care products will be monitored more closely by the Department of Justice. It may seem like good business sense to reach out to a competitor to see if they are experiencing similar issues with their supply chain or workforce, or whether they are contemplating raising prices. Resist this temptation. Information regarding a company's supply chain, costs and pricing is competitively sensitive information that should not be discussed with a competitor.

Final Thoughts

Businesses should expect that states are going to be vigilant in pursuing any perceived price gouging. Given the current media attention on medical masks and hand sanitizers, companies thought to be engaged in price gouging will not escape scrutiny. If other states follow California's lead, businesses should also expect that price gouging laws will be effective for much longer periods of time than those contained in the applicable laws. Because the legal landscape for price gouging is varied, businesses must be careful, particularly if they operate nationwide.

For more cutting-edge perspectives on the legal and business implications of COVID-19, visit our COVID-19 resource hub.

1. *People v. Two Wheel Corp.*, 525 N.E.2d 692, 694 (N.Y. 1988).
2. *See, e.g.,* "Directorate for Financial and Enterprise Affairs Competition Committee Working Party No. 2 on Competition and Regulation Excessive Prices – Background Paper" (Jan. 9, 2012) (Twenty-nine states and the District of Columbia prohibit excessive pricing of motor fuels and other commodities during periods of abnormal supply disruption), https://www.justice.gov/atr/public/international/278823.pdf; Price Gouging Laws by State, FindLaw, https://consumer.findlaw.com/consumer-transactions/price-gouging-laws-by-state.html.
3. Other states that set a 10 percent threshold include Arkansas, New Jersey, Oklahoma, West Virginia, and the District of Columbia.
4. Fla. Stat. Ann § 501.160.
5. Cal. Penal Code § 396, Louisiana follows a similar method.
6. Iowa (7 days), Alabama and Florida (30 days), Washington D.C. (90 days).
7. *See e.g.* Cal. Penal Code § 396, Connecticut General Statutes § 42-230, Ark. Code Ann. § 4-88-301 ("Selling commodities, household essentials, fuel, etc."); Fla. Stat. Ann § 501.160. ("Selling commodities, household essentials, rentals, fuel, etc."); N.Y. Gen. Bus. Law § 396-r. (Selling "goods and services vital and necessary for the health, safety and welfare of consumers"); N.C. Gen. Stat. § 75-38 ("Selling or renting goods and services "used to preserve, protect, or sustain life, health, safety..."); W.V. Code § 46A-6J-1 ("selling consumer food items, medical supplies, heating oil, building supplies").
8. *See e.g.* 2006 Pa. Laws 133 ("sell the goods or services within the geographic region that is the subject of the declared emergency"); La Rev.Stat. § 29:732 ("Selling goods/services") Haw. Rev. Stat. Ann. § 127A-30 ("the selling price of any commodity").
9. Alaska, Arizona, Colorado, Delaware, Maryland, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Mexico, North Dakota, Ohio, South Dakota, Wyoming, and Puerto Rico.
10. *See People v. AGIP Gas, LLC*, 2013 NY Slip Op 32805[U], *4 (Sup. Ct. Oct. 18, 2013) (a gas station owner successfully justified a temporary 80% price increase in the wake of an abnormal market disruption from Hurricane Sandy as resulting from supplier increases and "additional burdens and costs, including man-hours, which it incurred relating to gas lines, security concerns, crowd and traffic flow, uncertainty with respect to the delivery of replacement inventory, and other "soft costs" due to emergency conditions.").
11. Fla. Stat. Ann § 501.160.

Contributors

GRETCHEN L. JANKOWSKI

MELISSA M. IHNAT

Related Services & Industries

ANTITRUST & TRADE REGULATION
CORONAVIRUS (COVID-19)
LITIGATION

Related Keywords

COVID-19 (CORONAVIRUS)
RETAIL

Flexibility and Vigilance: Effectively Manage Government and Internal Investigations During COVID-19

APR 24 2020

Introduction

As a direct result of the COVID-19 pandemic, employees of many companies and government agencies are working remotely. This, however, has not necessarily resulted in a slowdown in either internal or government investigations. Nor should it provide a false sense of security to companies and other entities engaged in investigations prior to the outbreak of the coronavirus. Indeed, this is not a time for corporations to let down their guard in the conduct of investigations.

Since the outbreak, most U.S. enforcement agencies and regulators have been clear that corporate investigations will continue during the COVID-19 crisis, and that the government will continue to commence new investigations. Because most entities are operating remotely, they should be prepared, as the government is, to leverage technology as a substitute for typical in-person investigation-related activities. Importantly, while modern technology makes remote investigations manageable, there are key best-practice considerations that will assist companies and other entities in preserving the independence, confidentiality, and integrity of such inquiries.

Investigative Agency Responses to COVID-19

The COVID-19 crisis has certainly had a unique impact on individual U.S. enforcement agencies and regulators. For example, some federal investigative agencies, such as the Federal Bureau of Investigation (FBI), while operating primarily within a remote platform, are functioning more or less normally. Other agencies are de-prioritizing investigations that do not relate to the current health crisis, as employees and other resources are understandably redirected at an unprecedented level. Further, agencies led by more explicitly political actors, such as state attorney general offices, are more likely to shift their near-term focus to matters related to COVID-19. The same is true for agencies that include healthcare issues as part of their regular investigative portfolio.

Even for many investigations that are proceeding, the pace has diminished, or will likely soon slow, given the practical issues related to remote work and the increasing number of court closures. As a result of these new realities, several enforcement agencies and regulators have announced changes in the way they are handling investigations in the throes of COVID-19.

The U.S. Department of Justice (DOJ), the nation's most prominent collection of federal enforcement agencies, recently asked Congress for certain temporary emergency powers during the pandemic, including the ability to delay court proceedings, toll statutes of limitations, and expand the use of videoconferencing. The full extent to which Congress is receptive to such requests remains to be seen, but this highlights the realities facing many agencies. The DOJ is also prioritizing the investigation of misconduct allegations related to the COVID-19 outbreak, including, but not limited to, allegations of fraud, price gouging, and hoarding of critical supplies.

For its part, the Securities and Exchange Commission (SEC) has extended various filing deadlines, but is encouraging companies to be proactive and consider the need for COVID-19-related disclosures within the context of federal securities laws and the SEC's principles-based disclosure system. The SEC emphasized that it is only with exposure to these types of disclosure that investors can make informed decisions. The SEC also reminded the public of the importance of refraining from engaging in trading prior to the dissemination of material, non-public information.

The Federal Trade Commission's (FTC) Bureau of Competition has also announced that it is conducting a matter-by-matter review of its investigations and litigation efforts to consider modifications of statutory or agreed timing. The FTC advised that its investigators will be reaching out to parties to discuss these modifications and also encouraged parties and their counsel to proactively reach out to FTC staff to discuss these issues. Like the DOJ, the FTC is also likely to prioritize investigations involving deceit and fraud related to the COVID-19 pandemic.

The Financial Crimes Enforcement Network (FinCEN) has requested that financial institutions impacted by COVID-19 contact it and other regulators "as soon as practicable" with any concerns about their ability to timely file requisite Bank Secrecy Act (BSA) reports. Financial institutions are encouraged to keep FinCEN and their functional regulators informed as circumstances change. As with the DOJ and FTC, FinCEN is actively monitoring potential illicit activities connected to COVID-19, including imposter scams, investment scams, product scams, and insider trading.

The Consumer Financial Protection Bureau (CFPB) has likewise advised that it will work with affected financial institutions in scheduling examinations and other supervisory activities to minimize disruption and burden. And as the COVID-19 situation continues to develop, additional agencies will likely announce modifications to their operations.

Strategies for Conducting Remote Internal and Government Investigations

Attorney-Client Privilege and Work Product

A telephone or video interview provides corporations and other entities with far less control over who is present during (or listening to) an interview. Without appropriate security (and related encrypted) measures, such interviews create serious concerns with respect to "waiver" of confidentiality, the attorney-client privilege, and work product.

As a general rule, the attorney-client privilege is waived if a third-party is present during the communication. Though an interviewer may not ultimately be able to control what the interviewee does, he or she should explain at the outset of any investigation interview the importance of confidentiality and set forth clear and unambiguous instructions with respect to the potential ramifications of the presence of third parties, such as family members or cohabitants, present in the same room as an interviewee. To ensure maximum security, use one of many secure and encrypted audio/video software options.

The prevalence of smart speakers and digital personal assistants using artificial intelligence (AI) technology may also have privilege implications. There have been documented instances in which these devices have been "listening" to conversations -– unbeknownst to the participants. Accordingly, interviewers should be sure to remind interviewees to disable and unplug any such devices prior to an interview.

Document Collection and Review

Document collection efforts have also been noticeably impacted by the COVID-19 pandemic. While most electronic data can be collected remotely, in many investigations, whether internal or government-driven, there will be instances where it is necessary to collect physical documents. As a threshold matter, therefore, companies must be aware of government-mandated travel restrictions or other directives before engaging in a physical collection. And depending on the severity of the restrictions, which are frequently updated, physical collection of documents may simply not be possible at the current time. However, to the extent a physical collection can (and must) occur, normal best-practice principles apply, with certain additional considerations to heed.

Many employees are now working remotely, and companies are having to furlough or release employees. Accordingly, custodians may not be readily available to answer questions that could arise during the document collection process. It is therefore vital for companies to be organized and conduct custodian interviews as soon as an investigation commences to determine where relevant information is stored or maintained. Also, remember to obtain passwords and any other information concerning access to files at the outset. Further, communicate openly and regularly with the information technology department to get directory maps for available electronic databases.

Interviews

Remote investigations during COVID-19 may require that witness interviews be conducted telephonically or by video conference. Unlike an in-person interview, both the witness and the interviewer may be

tempted to record an interview held by telephone or video. Recording a conversation without the knowledge or consent of other parties can have serious consequences.

While some states allow an individual to record a conversation with the consent of only one party, other states require the consent of all involved parties. Therefore, prior to recording any conversation, companies conducting investigations must be certain they are aware of state and federal laws relating to recordings. For in-person interviews, both parties are in the same physical location; however, for remote interviews, the parties will be in different jurisdictions. Companies should thus be sure they understand the recording laws of each jurisdiction prior to an interview. Failure to comply with these laws can result in the imposition of civil and/or criminal penalties.

Regardless of the jurisdiction, an interviewer should notify the individuals being interviewed at the outset whether the interview will be recorded. Similarly, an interviewer should ask the interviewee if he or she is recording the interview. Even if the interviewee denies that he or she is recording, the interviewer should nonetheless state that the company does not consent to recording.

Audio or video recordings of interviews may also create discovery issues in future litigation. While written notes of witness interviews are typically considered attorney work product and therefore generally not discoverable, recordings of interviews may not be subject to the same protections. In sum, companies should therefore cautiously consider whether a recording is advisable. As noted above, such recordings can, in certain circumstances, create considerable legal risk for entities, including with respect to state and federal wiretap laws.

Another crucial consideration for virtual witness interviews is to ensure that appropriate security is in place to prevent third parties from intentionally or inadvertently gaining access to the conference line or video. For example, the increased use of certain group video platforms that have become popular has highlighted security vulnerabilities as hackers and other malefactors have hacked or compromised meetings. Accordingly, incorporate all possible security measures for virtual investigation interviews, including password protections and tested encryption.

Reporting

In light of the pandemic, companies conducting internal or government-initiated investigations may need to report findings (to the board or a government investigative body, for example) virtually via telephone or video conference. As with witness interviews and other key investigation steps, all attendees should be reminded of the importance of privilege, work product, and confidentiality (as appropriate) and be provided with instructions about taking notes or disclosing findings to outside individuals. Further, any reports or materials shown or provided to attendees should be conspicuously branded as “Privileged and Confidential,” as necessary. For companies with active compliance programs, spotlighting the vigor of those programs should be built into the reporting process as a potential mitigation measure with respect to

penalties.

Investigation Resolution

Investigation settlement negotiations have also been impacted by the economic effects of COVID-19. Many companies, for instance, will struggle (even more so than normally) with whether to disclose potential wrongdoing to the government (and ultimately agree to a penalty or fine) when their financial health is increasingly uncertain. A company that is concerned about its ability to pay a fine or penalty should proactively raise the issue with prosecutors or regulators so the government is operating with all necessary facts relating to the entity's current financial health. This simple communication will help both parties facilitate a fair and reasonable resolution.

Best Practices for Conducting Investigations in the Throes of COVID-19

While the COVID-19 pandemic has inarguably impacted the conduct of both internal corporate and government-initiated investigations, these matters will continue to move forward, albeit in a modified format, with an enhanced use of modern technology, and, in some cases, relaxed timelines. Companies and other entities facing the daunting prospect of a current or future investigation in the midst of the pandemic are therefore encouraged to hew closely to the best practices discussed above in order to protect the efficiency, effectiveness, independence, and integrity of the investigation, including all of the following:

1. Develop, maintain, and regularly update your internal investigation policy and associated procedures. Your investigation policy should set clear protocols for conducting investigations and account for unforeseen circumstances, such as a national emergency.
2. Craft a thoughtful and comprehensive investigation plan at the outset of the inquiry. The plan should include a tailored scope, realistic timelines, and due consideration of the current crisis.
3. Maintain attorney-client privilege and work product protections by employing the secure and encrypted technology necessary to carry out investigative steps.
4. Contemplate availability of resources to customize an investigation, particularly as those resources may be depleted during COVID-19. As the DOJ has said, it is not productive to "look under every rock and pebble" or "aimlessly boil the ocean."
5. Conduct document collection and interviews in a manner that integrates the added protections needed during a pandemic, including consideration of travel restrictions and adherence to security and legal requirements for virtual interactions.
6. In a government investigation, maintain consistent communication with investigators and/or regulators, particularly in the midst of COVID-19, as this helps demonstrate cooperation – and may pay dividends during negotiations.
7. Similarly – and particularly as settlement discussions appear more likely – proactively alert investigators of developments related to COVID-19 that will impede or hinder the company's ability to meet deadlines or possible financial obligations.
8. Likewise, for any type of corporate investigation, update internal leadership and the board regularly,

highlighting how the outcome may affect company resources and finances as the pandemic unfolds and, ultimately, resolves – prepare stakeholders.

9. Do not assume that, due to the pandemic, you can put "pencils down" with respect to an internal or government investigation and focus solely on other concerns. The government expects functioning entities to continue to investigate possible illegalities, irrespective of COVID-19 – albeit with potentially-relaxed timelines.
10. Involve outside legal counsel in the process. These are difficult times and investigations, even outside the confines of a pandemic, are extremely daunting.

For more cutting-edge perspectives on the legal and business implications of COVID-19, visit our COVID-19 resource center.

Contributors

JOHN P. CUNNINGHAM
JASON R. PARISH
MARTIN J. AMUNDSON

Related Services & Industries

CORONAVIRUS (COVID-19)
CORPORATE COMPLIANCE
CRIMINAL DEFENSE & GOVERNMENT ENFORCEMENT
INTERNAL INVESTIGATIONS
INTERNATIONAL SERVICES
LITIGATION
WHITE COLLAR DEFENSE, COMPLIANCE & INVESTIGATIONS

Related Keywords

COVID-19 (CORONAVIRUS)

Prioritizing Risk: Sustaining Life Science Compliance Programs During the COVID-19 Crisis

APR 28 2020

The spread of COVID-19 has disrupted business operations at companies of all sizes (and most industry sectors), with life science corporations experiencing among the more severe impacts. As the COVID-19 pandemic continues on its path of havoc, and businesses confront increased uncertainty (for example, in workforce and fiscal concerns), legal and compliance officers at life sciences companies are grappling with myriad compliance issues and unique program monitoring challenges. Maintaining functionality, corporate integrity and compliance program oversight, while continuing to meet regulatory expectations, are issues compliance professionals are now dealing with daily.

Sustaining compliance program functionality, for example, in the throes of a widespread global pandemic, presents unique challenges for life science entities, many of which are highly regulated and beholden to a litany of government requirements. While it is impossible to predict the various obstacles that will make compliance program oversight increasingly difficult, the key is to focus on risk management. By monitoring risk and bringing consistent attention to the core principles of compliance, life science companies can preserve adequate program robustness and uphold regulatory responsibilities and reporting requirements.

The Challenge

With many employees working remotely during the pandemic, it is more difficult to monitor their actions, including those activities that could present severe compliance risk to life science companies. Even with modern oversight, monitoring, and auditing technology, this workforce separation creates gaps in communication and invites greater potential for aberrant (and even illegal) activities. Legal and compliance officers and their teams may not have opportunities for typical in-person communications and regular updates from various group leaders. Moreover, with so much new information surfacing daily as a result of COVID-19, it can be exasperating to decide where to focus compliance resources and attention.

A Proactive Approach

Despite these hurdles, preserving compliance program stoutness and mitigating the possibility of issues with (or negative attention from) relevant agencies and regulators is possible in the COVID-19 environment. It requires a proactive, communicative, and risk-adjusted approach, particularly in the life sciences sector, where a lot of attention is currently concentrated by the government, and where compliance remains essential. Legal and compliance departments at life science companies can manage the

various elements of an effective program, even in a global crisis, by adhering to core compliance principles, namely leadership, communication, risk assessment, policies and controls, training, and oversight.

Attending to Core Program Components While in Crisis

Leadership

Chief Executive Officers, Chief Financial Officers, General Counsels, Chief Compliance Officers, and other members of the C-Suite in the corporate leadership group, in coordination with the board (where one exists), should take the lead in reinforcing the critical importance of compliance at life science entities during the COVID-19 pandemic. Messaging that reinforces adherence to compliance requirements must come from the top and align with the compliance department's priorities and goals.

Indeed, in times like these, one of the most valuable practices life-science leadership can adopt is to ensure that they keep abreast of real-time developments with respect to the pandemic, and likewise adapt company culture to the changing industry landscape. This can be demanding because, among other things, information is evolving in real time. Ultimately, in order to protect the company, leadership must be aware of germane new legislation, executive orders, ordinances, and guidance proposed and implemented at the federal, state, and local levels to evaluate risk and craft tailored risk mitigation plans.

Compliance officers, in particular, should stay attuned, for example, to the Department of Health and Human Services (HHS) as well as the Centers for Disease Control and Prevention (CDC) and the National Institutes of Health (NIH), among other pertinent agencies disseminating key information, to ensure that key stakeholders and managers have the most current compliance information to disseminate to employees.

Communication

With potential disruptions to supply chains, reduced workforce communications, delayed project management guidance, technological issues affecting employees operating from home, diminished access to information and materials, and other changes to the work environment, life science employees will justifiably have countless questions and concerns for leadership. Compliance directors can help manage inquiries from employees relating to these new, everyday hitches by making themselves available to answer employee questions, even more so than normal. While this may seem paradoxical on its face during a national emergency, modern technology, including vast improvements in video conferencing, can facilitate the regular intake of individual employee inquiries, to ensure that consistent messaging on compliance strategy and faithful program observance continues across the organization.

Risk Assessment

For most life science companies, risk assessment is the most critical of the core compliance program components during a global crisis. In light of this, legal and compliance officers should evaluate evolving risk on a proactive, regular basis and allocate resources accordingly. Indeed, compliance professionals

should take the time to assess their most pertinent risks on a daily basis and appropriately distribute resources. Typically, this type of assessment may be initiated on a less frequent basis. But considering the rapidly evolving nature of the COVID-19 pandemic, compliance teams need real-time information, and must work together to triage their compliance efforts, particularly for concerns exacerbated by COVID-19.

For example, with employees working remotely, many companies are facing additional security threats from home networks, along with cybersecurity risks and a greater potential for deviant conduct with (or to) company equipment. Compliance departments should, among other things, collaborate with IT leaders to ensure that all corporate-related connections are secure. This is especially important for life sciences companies, where confidential and proprietary information is often a prominent part of the business enterprise and can be more easily compromised on an employee's home network.

Further, it is important to ensure that supply chains are not interrupted and, in cases in which they are, maintain contingency plans to minimize disruptions. For instance, China produces roughly 90 percent of pharmaceutical ingredients used by the life science industry. The impact of COVID-19 on China has created a domino effect of sorts, disturbing supply chains worldwide. The actualized impact of any potential supply chain disruption may not be felt until the coming months, making it vital for life science companies to understand their current supply chain and have procedures in place to allay any interruptions or shortages.

Recently the U.S. Food and Drug Administration (FDA) updated its policies to address medical and drug supply shortages during the COVID-19 pandemic. In an effort to combat drug shortages, for example, the FDA revised its list of extended-use dates, allowing some products to be used beyond certain labeled expirations. Consequently, by closely monitoring the risk of supply chain issues during the crisis, life science companies can position themselves to notify the FDA of anticipated shortages. And compliance professionals are particularly adept at evaluating risk, which empowers them during a crisis, to make reasonable efforts to ensure that vital corporate concerns, such as product supply, are not compromised.

Policies and Controls

In a crisis of this magnitude, life science compliance teams must also take the requisite time to locate, organize, and make existing policies and procedures conspicuous. Managers and employees will need access to guidance quickly during uncertain times, and having key policies and procedures at arm's length will help save time and eliminate ambiguity when making decisions. Now is also a good time for compliance departments to reevaluate by setting forth new guidance and updated policies and controls to reflect the current environment. Fresh policies and procedures can also help outmaneuver the potential negative consequences of COVID-19, such as sick leave issues, employee safety, and novel employment-related rules promulgated by federal and state lawmakers. Finally, any new policies or procedures – even if temporary for COVID-19 – must be properly disseminated to all applicable employees and departments.

Training

Also, importantly, with the constantly developing nature of COVID-19, it may be tempting to allow existing life science training programs to fall by the wayside. Compliance leaders, however, must find ways to keep employees engaged in training. Many companies today, for instance, have adopted e-learning programs employees can complete remotely. Using such technology will not only facilitate ongoing and essential training for management and employees, it can also serve as a communication vessel for compliance leaders to remind employees that, despite the COVID-19 outbreak, regulators expect training programs to continue.

Monitoring and Oversight

Monitoring employee activity is more difficult when the workforce is geographically fragmented, which dictates that life science compliance teams be more vigilant in their compliance program oversight efforts. Legal and/or compliance officers should check in with the board, leadership, and employees regularly, and use secure email, audio, and video technology to create regular touchpoints, virtual or otherwise, to check that stakeholders, from the board room to the mail room, are adhering to company policies and continuing to follow compliance program requirements and expectations. Teaming with internal audit professionals and leaders from other business areas of the corporation can make this task much less daunting.

Managing Current CIA or Related Requirements

Adding to the above demands, life science companies currently beholden to Corporate Integrity Agreements (CIAs) from HHS, or enhanced compliance program obligations from any number of other agencies will, for the most part, be expected to maintain those responsibilities. If, for some reason relating to the pandemic, compliance programs face financial, resourcing, or related challenges making certain heightened compliance requirements either impractical or, perhaps, impossible, legal and compliance leaders are responsible for proactively notifying the appropriate government entity to request, through suitable channels, a temporary relaxing of such obligations.

Maintaining Program Robustness During COVID-19

With the continued uncertainty of the coronavirus emergency, compliance teams at life science companies must be prepared for the murkiness that lies ahead for business operations and program devotion. While the spread of COVID-19 certainly presents challenges, maintaining compliance program efficacy is achievable. Compliance teams can also take advantage of the pandemic-related complications to evaluate what strategies work, which may assist in making their programs more efficient in a post-COVID-19 world.

Ultimately, life science companies that successfully navigate COVID-19's unprecedented landscape will be those that proactively attend to the essential compliance program components discussed above, prioritize pressing compliance risks for timely remediation, and strategically allocate resources. Adhering to certain best practices tailored to the demands of a national emergency, including the following, which are mined from compliance program fundamentals, can serve as a guiding light in the inherent darkness of a

pandemic:

1. Develop a plan to provide cohesive and consistent messaging to leadership and employees relating to both the upkeep and any necessary adjustments to your compliance program during the COVID-19 outbreak.
2. Stay proactively apprised of the continuous changes to relevant federal and state laws, regulations, legislation, and executive orders inspired by the pandemic.
3. Reassess pertinent operational, business, and compliance risks on a more frequent (preferably, daily) basis, and reallocate compliance program resources accordingly.
4. As a compliance professional, be accessible and available to answer employee and corporate leadership inquiries by leveraging audio and video technology.
5. Use lessons learned during the crisis to begin to develop longer-term compliance program improvements to help ensure that the compromising of vital business practices will be mitigated in the event of a future national emergency.
6. Ensure that all relevant policies, procedures, and controls are readily accessible, even in the wake of COVID-19, so that employees can quickly access guidance.
7. Continue to require that employees remain active in the company's training program, so existing training regimens do not lapse.
8. Plan and facilitate regular touch points with executives, the board, and employees using secure email, audio, and video technology to monitor compliance program adherence and remind appropriate leaders of required compliance resources.
9. Skillfully team with internal audit professionals and trusted leaders from other business units in the corporation to assist in overseeing the compliance program.
10. Continue to observe CIA obligations, or enhanced compliance program requirements from other government bodies; and if, due to COVID-19 complications, this becomes unmanageable, promptly notify the proper authorities.

For more cutting-edge perspectives on the legal and business implications of COVID-19, visit our COVID-19 resource center.

Contributors

JOHN P. CUNNINGHAM

TERRY M. BROWN JR.

Related Services & Industries

CANNABIS

CORONAVIRUS (COVID-19)

CORPORATE COMPLIANCE

FDA & BIOTECHNOLOGY

HEALTHCARE
INTERNATIONAL SERVICES
LIFE SCIENCES
LITIGATION
WHITE COLLAR DEFENSE, COMPLIANCE & INVESTIGATIONS

Related Keywords

COVID-19 (CORONAVIRUS)

Price Gouging and Hoarding During COVID-19: Preparation and Compliance as Congress Seeks to Fill Gaps in State Laws

MAY 6 2020

Currently, a specific federal price gouging statute does not exist, placing enforcement primarily within the purview of the states.[1] In the past, state price gouging enforcement has been effective in responding to natural and man-made emergencies where the impact is isolated to a specific locality and/or is relatively short-lived. But the COVID-19 pandemic is different in scope and duration and has exposed the gaps in existing state laws and in enforcement of those laws during a crisis of this nature. To address these gaps and respond to the country's concerns about the impact that supply shortages are having on essential goods needed by first responders (and by the American people), Congress is currently considering several price gouging bills. If Congress is successful, many businesses currently not subject to price gouging and hoarding statutes may find themselves in violation of one or more new federal laws.

Current State Laws Vary in Scope and Content

A majority of states have price gouging laws, although there is no uniformity among these state laws. While state price gouging laws are typically triggered when a state declares an emergency[2] or experiences a major market disruption,[3] these price gouging laws differ, for example, in scope and content. Some state price gouging statutes are broad,[4] prohibiting any business from raising prices on all goods during the state of emergency, while others target only essential goods being sold to consumers.[5] There are a few state price gouging laws that only regulate fuel and oil prices,[6] but the majority of state price gouging laws focus on direct retail sales to consumers of necessary goods.

Notably, not all states even have a price gouging statute. There are 16 states,[7] plus Puerto Rico, that do not currently have price gouging laws. Several of those states, such as Washington, plan to use their consumer protection laws to combat price gouging during COVID-19. Other states are presently pursuing legislation, and Governor Larry Hogan of Maryland issued an executive order using a recent expansion of executive power to address price gouging during the current crisis.

More than any other recent national emergency, COVID-19 has demonstrated that a federal structure is necessary to eliminate hoarding and shortages of essential goods—and also prevent price gouging of consumers and first responders in their search for essential goods and materials. Indeed, as comprehensive as a state statute might be, it cannot expand its reach to regulate sales of products to

consumers and first responders outside of the state.

Federal Efforts in the Wake of COVID-19

Recognizing the severity that price gouging and hoarding is having on this country, the federal government is looking for ways to address national shortages and significant price increases for essential goods like ventilators, PPE, masks, and disinfectants.

Executive Order 13910: Prosecuting Hoarders to Prevent Price Gouging

On March 23, 2020, President Trump issued Executive Order 13910 (EO 13910), "Preventing Hoarding of Health and Medical Resources to Respond to the Spread of COVID-19." EO 13910 invokes Sec. 102 of the Defense Production Act (DPA), which defines hoarding to include "materials which have been designated by the President as scarce materials or materials the supply of which would be threatened by such accumulation." EO 13910 addresses situations where significant quantities of designated materials are withheld from the marketplace with the purpose of creating or exacerbating a shortage to raise prices. EO 13910 may be an effective tool for *discouraging* price gouging, but is not available for actual price gouging *enforcement*.

Coordination by Federal Agencies

The Federal Emergency Management Agency (FEMA) and the U.S. Department of Health and Human Services (HHS) have been working with medical supply companies to allocate personal protection equipment (PPE) and supplies and ensure timely delivery of supplies of PPE to "hot spots" designated by the Centers for Disease Control and Prevention (CDC). To participate, medical supply companies apply for permission through an expedited process established in March by the Department of Justice (DOJ) and Federal Trade Commission (FTC) to allow collaboration between competitors without violating antitrust laws. The voluntary coordination and allocation of such supplies by these companies removes buyer competition and the potential up-bidding for supplies between buyers. The program also seeks to prioritize those most in need of supplies. While the allocation process may help prevent price gouging by minimizing up-bidding and desperation--circumstances that foster price gouging of PPEs and other supplies--it does not itself regulate price gouging.

Moreover, the National Center for Disaster Fraud (NCDF), the DOJ, and the Federal Bureau of Investigation (FBI) are coordinating with a variety of states to assist with the investigation and prosecution of a variety of COVID-19-related issues. The NCDF, established in the wake of Hurricane Katrina, coordinates available law enforcement and prosecutorial resources and is able to field and organize complaints. The coordination is allowing states to manage an often-overwhelming number of complaints, and assist in the investigation and enforcement of those complaints. While the NCDF is busy with organizational tasks, the FBI and DOJ are teaming with U.S. Attorneys' Offices and state agencies to create task forces[1] to address a variety of complaints during the pandemic, including price gouging. These

federal efforts supplement and enhance the ability of states to respond to and track gouging complaints.

Focus on Gaps in State Coverage

The gaps in coverage for price gouging result from the division of regulatory authority over commercial activities between the state and federal governments. The federal government has exclusive control over interstate commerce, and the states, through their police power, may regulate sales within their boundaries. Indeed, state laws that impose restrictions or burdens on commercial activities outside their boundaries risk being struck down as unconstitutional.[2] The most prominent gaps that exist from the absence of a designated federal price gouging statute relate to state procurement, interstate commercial activities, business-to-business commerce, and states with no price gouging regulatory scheme.

State Procurement

Governor Andrew Cuomo of New York recently highlighted the significant issue of states bidding against one another, resulting in purchases at excessive prices. Neither the New York nor the California price gouging statutes, for example, could be applied to negotiations to restrict pricing without exceeding each state's authority and interfering with interstate commerce. As such, any federal price gouging legislation should consider the extent to which state procurement of essential goods should be regulated nationally.

Interstate Commercial Activities

As with state-to-state procurement, transactions occurring between businesses in different states is generally governed by federal law, whereas retail sales to consumers within a single state are often within the scope of state law. Therefore, it is likely that a state prosecuting an out-of-state business for pricing offered to an in-state business would be deemed as interfering with interstate commerce. This is one primary reason why the majority of active state price gouging laws are limited to retail sales. As a result, there is currently a significant gap in the regulation of price gouging between companies in different states. Accordingly, federal price gouging legislation should seek to address interstate activities such as these and thereby fill the void that prevents states from constitutionally regulating interstate commerce.

Business-to-Business Commerce

Because the majority of state price gouging statutes regulate retail consumer transactions, state regulation of business-to-business transactions is less prevalent. The limited number of states governing wholesale or supply transactions also creates a significant gap in enforcement.

Federal Legislation Aimed at Filling the Gaps

Despite the above-referenced federal efforts at enforcement, price gouging persists because most relevant state laws are not designed to protect the purchase or procurement of critical goods like PPE by hospitals, medical facilities and offices, assisted living entities, and other types of institutions. Recognizing that a pandemic of this magnitude requires a multi-faceted approach, Congress is presently undertaking to

address price gouging, particularly as it pertains to business transactions not currently covered by state laws. Ultimately, the federal government hopes to fill the gaps in regulation and remedy the lack of uniformity in current state laws. Since the coronavirus outbreak, four bills have emerged from Congress to combat price gouging. Given the number of proposals and the difficulties presented by the current legal and commercial landscapes, it is possible that one of these bills will be fast-tracked by integrating it into one of the COVID-19 financial support bills under consideration.

H.R. 6472

H.R. 6472, the "COVID-19 Price Gouging Prevention Act" sponsored by Representatives Janice Schakowsky, Frank Pallone, David Cicilline, and Jerrold Nadler is limited to the "duration of a public health emergency… as a result of confirmed cases of 2019 novel coronavirus." H.R. 6472 makes it unlawful for "any person to sell or offer for sale" a "good or service" at "unconscionably excessive" or "unreasonable" prices. The terms "unconscionably excessive" and "unreasonable" are not defined. Goods and services, however, are defined as "a good or service offered in commerce" including, but not limited to, necessities, PPE, medical supplies, and respirators. The bill compares prices currently offered to those offered by the company or a similarly-situated competitor "during the 90-day period immediately preceding January 31, 2020"--or "during the same 90-day period of the previous year" -- to determine whether the price is "unconscionably excessive" or "unreasonable." Violations of H.R. 6472 will be treated as an "unfair or deceptive act or practice in violation of a regulation under section 18 of the FTC Act" and enforceable by the FTC and state attorneys general. Penalties are civil rather than criminal and include fines and restraining orders. Further, H.R. 6472 does not supersede or preempt any state laws. H.R. 6472 applies to interstate commerce and is not limited to retail, consumer, and household goods. Unlike some of the other proposals, H.R. 6472 concerns only the COVID-19 pandemic and would not, as currently drafted, apply to unrelated national emergencies.

H.R. 6264

H.R. 6264, sponsored by Representatives Jason Smith and Josh Gottheimer and titled "Preventing Pandemic Profiting Act," if passed, would apply to the current pandemic and any declared future state of emergency. The bill makes it unlawful to offer or charge "an unconscionably excessive price" on "any goods or services identified by HHS as "vital and necessary for the health, safety, and welfare of consumers, including medical treatment." Under H.R. 6264, excessive pricing is "a price higher than the average price at which goods or services were sold or offered for sale during the 30-day period prior to the date on which a state of emergency declaration is made." H.R. 6264 relies on HHS to determine the scope of products covered by the Act and refers to pre-emergency pricing when determining whether the price is "unconscionably excessive." Violating H.R. 6264 is "a misdemeanor punishable by imprisonment in a county jail for a period not exceeding one year, or by a fine of not more than ten thousand dollars ($10,000), or by both that fine and imprisonment." As drafted, H.R. 6264 would fill the gaps in price gouging regulation, but only with regard to those goods and services identified as "vital" by HHS.

S. 3574

S. 3574, sponsored by Senator Thom Tillis and entitled "Ending Price-Gouging During Emergencies Act," is similar to H.R. 6264. S. 3574 would apply when a national emergency has been declared and FEMA issues a proclamation. According to the bill, FEMA may "issue a proclamation with respect to an emergency area during an emergency period to designate the goods and services" that will be governed by the bill. Thus, FEMA is responsible for the identification of goods and services covered by the bill, meaning that the emergency will define the scope of goods covered. Any person or company charging a price that "grossly exceeds" the item's average price from the month before the national state of emergency violates S. 3574. This bill imposes civil and criminal penalties "up to 10 times the amount of profits from price gouging, with maximum criminal penalties up to $500 million." Enforcement of this bill is the responsibility of the FTC and affords state attorneys the ability to prosecute after they provide notice to the FTC of their intent to enforce, at which time the FTC may intervene or leave enforcement to the state. S. 3574 would fill gaps in price gouging regulation, but only with regard to those goods and services identified by FEMA. S.3574 does not preempt state laws, and as such requires compliance with the variety of state laws in addition to the new federal requirements. By allowing penalties "up to ten times the amount of profits," S. 3574 has the harshest penalty profile of any of the proposed bills.

H.R. 6450

H.R. 6450, sponsored by Congressmen Joe Neguse and Ted Lieu, is titled "Price Gouging Prevention Act." The legislation is triggered by either a national emergency or an "abnormal disruption in the market" ("abnormal disruption" is not defined). The proposed bill covers "consumer goods." However, the bill appears to expand the scope of goods covered beyond "consumer" or retail sales to end users because the definition of "consumer good" here is "a good offered in commerce." This broad definition could, for instance, encompass sales throughout supply chains, business-to-business transactions, and state procurement. The enforcement of this bill is the concern of the FTC, similar to H.R. 6472. A violation of the bill is considered an unfair or deceptive act or practice enforceable under the Federal Trade Commission Act (15 U.S.C. 57a (a)(1)(B)). The bill also provides for enforcement by states after they provide notice to the FTC of their intent to enforce, at which time the FTC may intervene or leave enforcement to the state. Penalties for violation here are civil rather than criminal and include fines and restraining orders. The bill does not preempt the existing patchwork of state laws. Therefore, while the bill will address many of the gaps, it does not create a uniform, national price gouging law.

While the proposed federal legislation described addresses the most serious price gouging issues related to COVID-19, none of these proposed bills preempts current state gouging laws. Without preemption, companies operating on an interstate basis and seeking to comply with a litany of diverse state statutes face continued compliance challenges, for which preventive measures will prove particularly useful.

Preventive Measures for Businesses

Price gouging laws and regulations are being primarily enforced at the state level, although it is only a matter of time before heightened federal enforcement. As federal efforts at legislation continue, and state

enforcement surges, businesses should be cognizant of current gaps in applicable state laws, monitor federal efforts to seal those gaps, and implement (or enhance) preventive measures to deter, detect, avoid, and, if necessary, effectively respond to gouging and hoarding enforcement actions.

Familiarize Yourself with Applicable State Laws

None of the proposals in Congress to establish price gouging and/or hoarding laws and regulations will displace current state laws. And even if a federal statute were enacted that preempted one or more state laws, state price gouging laws have been active and enforceable since the COVID-19 crisis unfolded. Accordingly, as part of ongoing efforts to assess risk and allocate available compliance resources, companies should assign internal legal and compliance teams with responsibility for reviewing and monitoring state laws (and federal legislation efforts) as the COVID-19 pandemic continues.

Maintain Strong Messaging from Leadership

COVID-19 has created substantial challenges for businesses attempting to move forward in a marketplace and economy currently rife with uncertainty. Nevertheless, leadership, whether through the Board, the C-Suite, management personnel, or a combination of all three, should step forward, as resources permit, to maintain strong messaging with employees on the importance of following key guidelines, policies, and procedures relating in any way to mitigating price gouging and hoarding risk.

Be Proactive and Act Now

Do not wait for Congress to pass federal legislation before taking preventive measures. Because each company's current prices will be compared to its pre-pandemic pricing, its pricing activity from the start of the pandemic is subject to scrutiny under any of the proposed federal bills. Conduct regular auditing, monitoring, and oversight of your pricing models and keep your compliance and legal teams in the loop.

Report and Memorialize Pricing Changes

Be prepared to justify and appropriately memorialize the legal and economic rationales for any actual or proposed price increases. Generally, an increase in price reflecting current market circumstances – for example, growing shipping costs, limited labor supply, burgeoning material costs, and supply chain price increases –is potentially a defense to price gouging allegations. Therefore, track all pricing variations, cost increases, and reports reflecting the changing status of the supply and production markets.

Update Relevant Policies and Procedures

A review of almost all federal and state enforcement and regulatory agency guidelines reveals that one of the keys to maintaining a robust compliance program, particularly at a time like now where more infrequent risks such as price gouging and hoarding become amplified, is to appropriately update pertinent policies and procedures. As resources permit, evaluate applicable policies and protocols and, if necessary, integrate corporate gouging and/or hoarding guidelines.

Remain Vigilant in Business Partner Engagements

Remember, antitrust laws still apply. If you plan to cooperate with competitors in response to state or federal requests, be sure to seek and obtain permission from the FTC and DOJ. Any unapproved communications with competitors makes a company potentially vulnerable to conspiracy allegations in violation of antitrust laws, putting the company at further risk for attention by federal regulators.

No News Is Not Necessarily Good News

Just because a company has not yet been notified about a suspicious price increase or hoarding allegation does not mean that it is immune to a potential enforcement action. A significant portion of price gouging inquiries will likely take place after the pandemic since many courts are currently unable to assemble grand juries for criminal indictments and state and federal law enforcement resources are stretched thin. Maintain price discipline and oversight throughout the crisis and set applicable compliance guidelines to avoid future brush-ups with either federal or state enforcement agencies.

Do Not Hesitate to Seek Help and Guidance

These are extremely challenging times for companies of all types, and particularly those involved in the purchase or sale of PPEs and other materials that are less available as a result of the pandemic. There are documented instances (since the outbreak of COVID-19) of agencies and regulators – including the DOJ, FEMA, DOJ, HHS, SEC, and relevant state entities – providing skillful guidance to companies that need assistance in complying with applicable gouging and hoarding expectations and requirements. It may also be useful to involve outside legal counsel, as many law firms have specialized price gouging expertise to lend a hand to companies in need of advice during such a difficult national emergency.

For more cutting-edge perspectives on legal and business implications of COVID-19, visit our COVID-19 resource center.

---

1. The federal government does, however, work closely with certain states to team on enforcement issues.
2. *E.g.* California (CA Penal Code § 396); Georgia (GA Code § 10-1-393.4); Pennsylvania (73 Pa. Stat. § 232.4).
3. *E.g.* Maine (10 ME Rev Stat § 1105); New York (GBS § 396-r); North Carolina (N.C. Gen. Stat. § 75-38).

4. *E.g.* Alabama (Ala. Code §§8-31-1 thru 8-31-6); Mississippi (MS Code § 75-24-25); Oklahoma (15 OK St. §§ 777.1 thru 777.5).
5. *E.g.* California; Florida (FL Stat § 501.160); New York; Rhode Island (RI Gen L § 6-13-21); Texas (Tex. Bus & Com. Code §17.46(b)(27)).
6. *E.g.* Illinois (Ill. Admin. Code tit.14, §§ 465.10 thru 465.30); Indiana (IN Code § 4-6-9.1-2); Vermont (9 V.S.A. § 2461d).
7. Alaska, Arizona, Colorado, Delaware, Maryland, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Mexico, North Dakota, Ohio, South Dakota, Washington and Wyoming.
8. Nevada, Kentucky, Virginia, and West Virginia have each launched joint task forces.
9. *See, e.g. Ass'n for Accessible Meds. v. Frosh*, 887 F.3d 664, 670 (4th Cir. 2018) (Maryland law aimed at preventing price gouging of essential off-patent and generic drugs was struck down as violating the dormant commerce clause

Contributors

GRETCHEN L. JANKOWSKI

JOHN P. CUNNINGHAM

MELISSA M. IHNAT

Related Services & Industries

ANTITRUST & TRADE REGULATION

CORONAVIRUS (COVID-19)

CORPORATE COMPLIANCE

FDA & BIOTECHNOLOGY

HEALTHCARE

LIFE SCIENCES

LITIGATION

WHITE COLLAR DEFENSE, COMPLIANCE & INVESTIGATIONS

Related Keywords

COVID-19 (CORONAVIRUS)

The Foreign Corrupt Practices Act In The Age Of COVID-19

MAY 27 2020

2020 FCPA Enforcement Actions Suggest Industries Hit Hardest by Coronavirus May Face Increased Risk of Exposure to Anti-Corruption Enforcement

Introduction

As countries across the globe begin lifting the social and economic restrictions put in place to help "flatten the curve" of the COVID-19 pandemic, companies must remain vigilant in their compliance efforts as they attempt to recoup the massive economic losses suffered as a result of the crisis. In this challenging and uncertain time, it is perhaps even more important that all companies follow the DOJ and SEC guidance regarding the Foreign Corrupt Practices Act (FCPA) compliance and enforcement and that compliance programs be put in place or re-evaluated to make certain that a company will not run afoul of the FCPA. Written compliance procedures, in the form of a general code of conduct and specific anti-corruption compliance policies and procedures, along with strong company-specific risk assessments are necessary. A commitment to continued compliance from senior management along with the establishment of procedures regarding third-party due diligence, confidential reporting of potential violations, as well as for conducting effective internal investigations are of critical importance.

In April, the Asian Development Bank projected that the global costs of the Coronavirus could reach $4.1 trillion – nearly five percent of global gross domestic product.[1] While the full impacts of the COVID-19 pandemic remain largely unknown, one thing is certain – the virus has had, and will continue to have, a devastating impact on the global economy with the energy and oil, travel and entertainment, and healthcare industries bearing the brunt of that burden. Undoubtedly, as world economies begin to reopen, companies in these industries and others will face new challenges as they seek ways to recover the losses they have suffered to date.

In addition to the economic challenges facing companies across these market industries, a review of 2020 enforcement actions brought under the Foreign Corrupt Practices Act (FCPA) suggests that these same industries remain the focus of federal regulators. With mounting pressures to gain traction in the newly reopened global market and the ever-watchful eye of federal regulators, companies must design, implement, and enforce anti-corruption policies which may assist in ensuring that the desire to regain profits and market share is not satiated through unscrupulous means.

Energy / Oil

As citizens across the world shelter-in-place, the Coronavirus has had a devastating impact on the global demand for oil – with some experts suggesting the industry may never fully recover.[2] As 187 countries and territories enacted efforts to flatten the curve, the International Energy Agency expects global oil demand to fall by a record 9.3 million barrels per day in 2020.[3] This global lack of demand for crude oil, and its economic impact on energy companies, was only exacerbated by the temporary dispute between Russia and Saudi Arabia in the global oil market. In March, Russia refused to agree with OPEC's proposal to cut production amid the Coronavirus pandemic and, days later, Saudi Arabia slashed its April official selling price by $6-$8 per barrel. All of these forces working in unison to depress global oil prices led, in April, to prices turning negative with the price of a barrel of West Texas intermediate, the benchmark for US oil, falling as low as minus $37.63 a barrel.

Given the impact of the global decrease in oil prices and the threat of a prolonged recovery in the energy markets, companies are now faced with the question of when, and through which methods, their revenues and markets will stabilize and, perhaps, even rebound. To that end, compliance departments across the energy sector must ensure that their methods, policies, and procedures are thorough and rigorous.

This need for fulsome compliance policies and practices is highlighted by the recent FCPA enforcement action against Eni S.p.A., an Italian multinational oil and gas company, the FPCA charges brought by the SEC against former Goldman Sachs Executive Director Asanta Berko, the guilty pleas of Tulio Anibal Farias Perez and Armengol Alfonso Cevallos Diaz, and the sentencing of Juan Jose Hernandez Comerma. Each of these enforcement actions and guilty pleas suggest that federal anti-corruption regulators remain focused on the energy industry.

Travel and Entertainment

One of the industries hardest hit by the impacts of the Coronavirus – and the natural victim of countries in lockdown – is the travel industry. The U.S. Travel Association recently stated that the U.S. travel and tourism industry could lose upwards of $910 billion and 6 million travel-related jobs.[4] While nearly every travel-related sector of the economy – including auto-makers, vacation rentals, lodging, recreation and amusement – has seen the devastating impacts of the coronavirus, the airline industry, including the downstream manufacturers, have been hit particularly hard. With passenger counts dropping by 96

percent and airlines cancelling more than 70 percent of their flights, airlines around the world are seeking alternative means to avoid bankruptcy. In an attempt to assist in this process, the United States Congress passed the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) which included $58 billion to prop up the aviation industry.

The impacts of the decline in travel have also been felt by downstream business, including manufacturers. For example, Boeing reported a $641 million loss for the first quarter of 2020 and at its April 27, 2020 annual meeting, CEO David Calhoun told shareholders, "the health crisis is unlike anything we have ever experienced" and that "it will take two to three years for travel to return to 2019 levels and an additional few years beyond that for the industry's long-term growth trend to return."[5] All of these statements come as some of the largest airline manufacturers in the world – Boeing and McDonnell Douglas – halt production of commercial airliners and furlough workers until the pandemic subsides and/or a vaccine is developed.

The increased focus on the travel industry by federal regulators is perhaps best exemplified by the DOJ's recent settlement – the largest FCPA settlement in U.S. history – with an airline manufacturer that was able to enter into a deferred prosecution agreement.

As with the travel sector, COVID-19's economic impact has devastated companies across the entertainment industry including, but not limited to, cruise lines, movie theaters, concert venues, amusement parks and, notably, sports. Beginning in early March, major sporting leagues – including the NBA, PGA, NHL and MLB – both in the United States and across the globe have seen their seasons postponed or cancelled in an effort to avoid the large gatherings that accompany these sporting events and curb the further spread of the virus. In addition to these closures and postponements, on March 24, 2020, Japanese Prime Minister Shinzo Abe and Olympic Committee President Thomas Bach agreed to postpone the 2020 Summer Olympics in Tokyo to 2021 – marking the first time that the Olympic Games have been postponed or cancelled other than during the course of a world war.

In addition to the cultural impacts that the loss of live sporting events has had on the global conscious, the closure of major sporting leagues and the postponement of the 2020 Olympic Games has had a devastating financial impact for both the leagues themselves and the broadcasters and marketers which rely on these events to reach potential clients. By way of example, the organizers of the Tokyo Olympics estimate the cost of the delay at approximately $12.6 billion, while other experts claim that number to be closer to $25 billion. These figures include the billions of dollars spent by sponsors and broadcasters on the Games. Additionally, financial experts have estimated the cost of cancelling the remainder of the NBA season at approximately $650 million in ticket and non-ticket revenue to the league – with the potential loss of television and marketing rights for March Madness alone to total approximately $870 million dollars.[6]

With such staggering figures, the ground remains fertile for potential FCPA violations as sponsors and organizers attempt to regain some of the financial ground they have lost. This is perhaps best exemplified

by the April 6, 2020 indictment of two former 21st Century Fox Inc. executives, a former co-CEO of Sanish media company Imagina Media Audiovisual SL, and Uruguayan sports marketing company Full Play Group S.A. for their alleged role in the long-running corrupting investigation surrounding the Fédération Internationale de Football Association (FIFA).

Healthcare

While FCPA enforcement actions in the healthcare industry are not novel (*e.g.*, Fresenius Medical Care, Johnson & Johnson), the flurry of activity in this sector due to COVID-19 likely increases the FCPA risk exposure for healthcare providers, medical device companies, and pharmaceutical companies.

As the healthcare industry around the world rushes to develop therapeutics and a potential vaccine for the Coronavirus, it is vital that companies implement, maintain, and enforce their anti-corruption policies and procedures in an effort to avoid potential FCPA risks. This exposure is driven in large part by the federal agencies enforcement theory that employees (*e.g.*, physicians, nurses, lab personnel) of certain foreign health care systems are considered to be "foreign officials" under the FCPA. The effects of the broad enforcement theory are on full display in the SEC's recent FCPA enforcement action against Cardinal Health, Inc. for allegedly directing certain marketing funds to Chinese government-employed healthcare workers and state-run retail companies who had influence over purchasing decisions.

Conclusion

As countries and economies across the world begin to reopen, compliance departments must remain vigilant as those sectors hit hardest by the economic impacts of the COVID-19 pandemic now seek to recoup their economic losses. Strong compliance policies and procedures become even more critical as 2020 FCPA enforcements, indictments, and sentencings show that federal regulators remain focused on the travel and entertainment, energy/oil and healthcare sectors.

To this end, it is important that all companies follow the DOJ and SEC guidance regarding FCPA compliance and enforcement and that any compliance program include, among other elements:

Written compliance procedures, in the form of a general code of conduct and specific anti-corruption compliance policies and procedures;

- Strong company-specific risk assessments;
- Commitment to continued compliance from senior management;
- Procedures regarding third-party due diligence;
- Procedures and processes to allow and encourage confidential reporting of potential FCPA violations; and
- Procedures for conducting internal investigations.

For more information on the FCPA implications of the COVID-19 recovery or for assistance in addressing your FCPA compliance, Buchanan's white collar defense, compliance & investigations professionals are here to assist.

For more cutting-edge perspectives on legal and business implications of COVID-19, visit our COVID-19 resource center.

---

1. https://time.com/5814933/coronavirus-pandemic-cost-4-trillion/
2. https://www.cnn.com/2020/04/29/economy/oil-demand-peak/index.html
3. *Id.*
4. https://www.forbes.com/sites/tamarathiessen/2020/04/01/us-travel-industry-warns-of-910b-coronavirus-losses/#2151b4cf6c9d
5. https://www.npr.org/sections/coronavirus-live-updates/2020/04/27/846819966/boeing-ceo-sees-years-of-recovery-from-coronavirus-ahead-for-aviation-industry
6. https://www.statista.com/topics/6098/impact-of-the-coronavirus-on-sport/

Contributors

MICHAEL J. ENGLE
JORDAN A. YEAGLEY

Related Services & Industries

CORONAVIRUS (COVID-19)
ENERGY
HEALTHCARE
LITIGATION
WHITE COLLAR DEFENSE, COMPLIANCE & INVESTIGATIONS

DOJ's Latest Guidance Further Clarifies Factors for Evaluating Compliance Programs

JUN 16 2020

Earlier this month, the Criminal Division of the U.S. Department of Justice ("DOJ") published a revised version of its guidance document entitled "Evaluation of Corporate Compliance Programs" ("Updated Guidance"). This is an update from prior versions, originally issued in February 2017 ("Original Guidance") and amended in April 2019 ("Amended Guidance"), and maintains the DOJ's stated commitment to regularly provide fresh compliance advice to nourish an eager corporate defense bar.

The Updated Guidance does not reflect a significant change in the DOJ's overall views, expectations, or practices with respect to the evaluation of compliance programs. Instead, it provides some enhanced recommendations and related advice based on the DOJ's recent experience assessing programs and constructive feedback from the business community and compliance and investigation professionals.

Consistent with prior DOJ compliance guidance releases, the U.S. Sentencing Guidelines, and the Justice Manual (outlining the principles for the DOJ's prosecution of companies), the Updated Guidance spotlights three "fundamental questions" federal prosecutors should ask in examining compliance programs, with the goal of determining whether the programs have a sturdy infrastructure, necessary resources, and a cooperative culture -- all of which are essential to maintaining an effective program:

- Is the corporation's compliance program well designed?
- Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?
- Does the corporation's compliance program work in practice?

As the DOJ explains in the Updated Guidance, ultimately, the new document tasks prosecutors with endeavoring to understand why companies set up their compliance programs the way they do, and how such entities efficiently facilitate the meaningful, customized improvement of those programs over time.

Overview of the Updated Guidance

The Updated Guidance spotlights the need for companies to employ programs that are dynamic, tailored, and consistently assessed to account for evolving corporate risks – rather than reflective of mere "snapshots" in time. This overarching theme includes a notable modification to the DOJ's prior view on the ongoing maintenance of compliance programs, focusing even more acutely now on whether programs are

adequately resourced, regularly monitored, and operating effectively at all levels.

With the Updated Guidance, the DOJ also emphasizes its commitment to a reasonable, individualized, and flexible approach to assessing compliance programs, which considers each company's unique circumstances within the framework of existing program expectations, including size, industry sector, global footprint, regulatory landscape, and other factors related to the company's operations.

In terms of program specifics, the Updated Guidance adds expectations relating to the following: (1) enhanced access to (and use of) relevant data; (2) shrewd allocation of compliance resources; (3) improved checks and balances for training; (4) vigilant management of third-party and merger and acquisition risks; and (5) mindfulness of the intrinsic value of corporate benchmarking.

Thoughtfully attending to the clarifications in the Updated Guidance and integrating reasonably scoped and commensurate program modifications (based on the revised advice) will help corporations and other entities mitigate evolving compliance risk and tactfully prepare their programs for scrutiny by the DOJ's flexible evaluation methodology in the event they are subject to a corporate enforcement action.

Principal Revisions in the Updated Guidance

Enhanced Data Gathering, Analysis, and Usage

Perhaps the most prominent revision and area of focus in the Updated Guidance pertains to the DOJ's recommendation that compliance programs be functionally dynamic, with a risk assessment process designed to frequently gather relevant data, analyze it, and utilize the data in a manner that informs regular, customized program enhancements – rather than relying on static risk assessment procedures premised on what the DOJ terms mere "snapshots" in time.

This focus on data-driven analysis is also represented in the section of the Updated Guidance addressing compliance resourcing and program monitoring and testing. For example, the Updated Guidance counsels that "control personnel" within the corporate compliance structure should have sufficient access to relevant sources of data to allow for timely and effective monitoring and testing of policies, procedures, controls, and financial transactions. Similarly, with respect to testing compliance program efficacy, the DOJ encourages the regular collection and examination of compliance data.

The DOJ understands that such data is enormously valuable in determining program success, including, for example, in examining incoming and outgoing company payments. Consistent monitoring of payment data can help capture inconsistencies and "exceptions" that may signify trouble, not only with respect to illicit activity, but also in terms of compliance program effectiveness. Further, the government notes in the Updated Guidance that it may credit a risk-based program that devotes apt attention and resources to data from high-risk transactions, even when this fails to avert an infraction.

Improved Compliance Resourcing

Ensuring adequate compliance resourcing and the hiring and training of skilled compliance personnel are consistent themes emanating from the DOJ in its various compliance guidance materials. The Updated Guidance continues this theme, with a major focus on alerting companies to ensure their compliance programs are not only sufficiently resourced, but also fully accessible to employees. Indeed, it instructs prosecutors to identify how and where corporations publish their policies and procedures, track when they are accessed to determine which policies are receiving the most attention, and ensure that employees have the tools needed to review and comply with these standards.

This instruction reveals DOJ's concern that compliance program requirements are actually followed in practice by employees, managers, and C-Suite executives. Put another way, the DOJ has great disdain for "paper tiger" programs with standards and controls that may read well in a conference room, but have little practical application and are generally ignored by, or inaccessible to, company personnel.

One of the keys here for companies seeking to meet the DOJ's expectations in the compliance resourcing area is to grant appropriate authority to those responsible for compliance so they have direct and independent access to the company's governing authority (or an appropriate subgroup). With such access, compliance leadership can regularly report to the brass on compliance incidents, elicit relevant feedback from corporate executives, and pitch, as appropriate, for additional funding, more experienced compliance personnel, and a seat at the C-Suite table for input on corporate decision making.

Appropriately Customized Training

The Updated Guidance also includes a significant amount of innovative information about the DOJ's view of effective training, including an emphasis on the use of data (discussed separately above) to assess whether training has impacted compliance program adherence by corporate personnel. For example, data indicating repeat offenders and an increase (or decrease) in compliance incidents or illegalities over time can be used to determine whether program enhancements have been impactful.

The DOJ also discusses the potential significance of shorter, more targeted training sessions to help keep the attention of employees while also enabling them to timely identify and raise issues to appropriate compliance, internal audit, and other risk management leaders. The DOJ is clearly concerned with whether employees are positioned to ask questions arising out of training sessions either online or in person through an accessible (and anonymous, if requested) communication channel (similar to the way a whistleblower hotline may be used to report compliance incidents in the field).

And the DOJ, as expressed in the Updated Guidance, has now openly articulated in writing its expectation that companies with the necessary means will devote time and other resources to train their compliance, audit, risk, accounting, and internal controls personnel. This makes good sense.

Attentive Management of Third-Party and M&A Risk

Predictably, the Updated Guidance reflects the DOJ's longtime focus on third-party risks and the expectation that companies robustly manage intermediary engagements both during the onboarding process and, perhaps more importantly, throughout the entirety of the engagement (via ongoing relationship monitoring and training, as necessary and appropriate). The DOJ also recognizes, however, that the need for, and degree of, suitable due diligence can vary based on a variety of factors, including, for example, the size and nature of the company, type of transaction, and third party.

Consistent with this guidance, the latest revisions make clear that federal prosecutors should gauge the extent to which a company knows the qualifications and associations of its third parties, including the business agents, consultants, intermediaries, and distributors commonly involved in corruption and related schemes to conceal misconduct (such as the offer or payment of bribes to foreign officials).

Therefore, companies are expected to determine and memorialize the business rationale for engaging any third party and gain a fulsome understanding of each third party's business relationships -- particularly with respect to foreign officials, who, for example, can create risk for companies under many criminal statutes, most notably the heavily enforced Foreign Corrupt Practices Act ("FCPA").

Similar to the DOJ's expectations for risk management relating to third parties, the Updated Guidance explicitly affirms prior statements by the DOJ that a properly constructed and functioning compliance program should include comprehensive due diligence of any acquisition targets, adding that there should also be "a process for timely and orderly integration of the acquired entity into existing compliance program structures and internal controls." As with third parties, the DOJ expects that companies will thoroughly evaluate targets prior to acquisition, whenever feasible, and then efficiently assimilate newly acquired entities, followed by post-acquisition monitoring and auditing.

Increased Consideration of Corporate Benchmarking

Finally, while somewhat more subtle, the DOJ, in the Updated Guidance, weaves in references to compliance benchmarking. In the section on risk assessments, the DOJ challenges companies to adopt a procedure for tracking and incorporating lessons learned from compliance issues experienced by companies operating in a similar industry sector and/or geographic region.

Along these lines, the Updated Guidance also encourages companies to examine, test, and improve its compliance program based upon lessons learned from the misconduct of other companies. Often called "benchmarking" in the compliance world, the DOJ's references to such comparative efforts in the Updated Guidance (in the context of program efficacy) evidences an acknowledgement of the importance of the practice and its intent to inquire into benchmarking when evaluating programs.

Conclusion: Inherent Value in Periodic, Updated Guidance

While the Updated Guidance does not substantially alter the playing field with respect to the DOJ's evaluation of corporate compliance programs, its considerable value lies in the elucidation of newly refined nuggets of practical guidance for compliance professionals based on the DOJ's real-world experience and, in DOJ parlance, "lessons learned" from the business, compliance, and investigation communities. These inputs from outside sources to DOJ, and the DOJ's consideration of same (in short order, considering the Amended Update in 2019 was issued just a little over a year ago), help foster a cordial compliance dialogue between the government and the corporate defense bar on issues of great importance for companies. The result is a meaningful compliance roadmap provided by the DOJ, revised on a regular basis, which corporations can use as a barometer to review, analyze, and measure their current compliance programs, with confidence that the DOJ is dedicated not only to evaluating, but also listening and learning. This will invariably encourage future updates by the DOJ addressing less-frequently discussed compliance topics, including those more germane to financial and controls issues.

Contributors

JOHN P. CUNNINGHAM
KODY M. SPARKS

Related Services & Industries

CORPORATE
CORPORATE COMPLIANCE
CRIMINAL DEFENSE & GOVERNMENT ENFORCEMENT
INTERNAL INVESTIGATIONS
INTERNATIONAL SERVICES
LIFE SCIENCES
LITIGATION
WHITE COLLAR DEFENSE, COMPLIANCE & INVESTIGATIONS

U.S. Department of Justice
Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530
March 24, 2020

TO: MEMORANDUM FOR ALL HEADS OF LAW ENFORCEMENT COMPONENTS, HEADS OF LITIGATING DIVISIONS, AND UNITED STATES ATTORNEYS

FROM: THE DEPUTY ATTORNEY GENERAL

SUBJECT: Department of Justice Enforcement Actions Related to COVID-19

As you know, we have seen an unfortunate array of criminal activity related to the ongoing COVID-19 pandemic. Capitalizing on this crisis to reap illicit profits or otherwise preying on Americans is reprehensible and will not be tolerated. I am issuing this Memorandum to inform you of the sorts of schemes that have been reported, to identify certain authorities that I am directing you to consider deploying against these schemes, and to emphasize the importance of state and local coordination during this difficult time.

I. REPORTED SCHEMES RELATED TO COVID-19

To date, the U.S. Attorney's Offices have received reports of individuals and businesses engaging in a wide range of fraudulent and criminal behavior. This includes:

- Robocalls making fraudulent offers to sell respirator masks with no intent of delivery;
- Fake COVID-19-related apps and websites that install malware or ransomware;
- Phishing emails asking for money or presenting malware;
- Social media scams fraudulently seeking donations or claiming to provide stimulus funds if the recipient enters his or her bank account number;
- Sales of fake testing kits, cures, "immunity" pills, and protective equipment;
- Fraudulent offers for free COVID-19 testing in order to obtain Medicare beneficiary information that is used to submit false medical claims for unrelated, unnecessary, or fictitious testing or services;
- Prescription drug schemes involving the submission of medical claims for unnecessary antiretroviral treatments or other drugs that are marketed as purported cures for COVID-19;

- Robberies of patients departing from hospitals or doctor offices;
- Threats of violence against mayors and other public officials; and
- Threats to intentionally infect other people.

You should be on the lookout for these sorts of schemes, as well as any others like them.

II. SPECIFIC AUTHORITIES TO PUNISH WRONGDOING RELATED TO COVID-19

Consistent with the Attorney General's March 16 Memorandum, I am directing your Offices to focus your attention on the following categories of offenses that may be relevant to the kinds of pandemic-related crimes we have seen reported.

First, we know that there are individuals and businesses taking advantage of the COVID-19 crisis to engage in fraudulent or otherwise illegal schemes. Depending on the specific facts, these acts may violate any number of provisions in Title 18. *See, e.g.*, 18 U.S.C. § 1341 (mail fraud); *id.* § 1343 (wire fraud); *id.* § 1030 (computer fraud); *id.* § 1347 (healthcare fraud); *id.* § 1349 (conspiracy to commit fraud); *id.* §§ 1028–1028A (identification fraud and aggravated identity theft); *id.* § 1040 (fraud in connection with major disasters and emergencies); *id.* § 2320 (trafficking in counterfeit goods).

Moreover, the sale of fake drugs and cures may be prohibited under Title 15, *see* 15 U.S.C. § 1263(a) (introduction of misbranded or banned hazardous substances into interstate commerce), constitute a violation of the Food, Drug, and Cosmetic Act, *see* 21 U.S.C. § 333 (introduction of misbranded or adulterated drug or device into interstate commerce), or constitute a violation of the Consumer Product Safety Act, *see* 15 U.S.C. § 2068 (sale, manufacture, distribution, or import of a consumer product or other product that is not in conformity with consumer-product-safety regulations).

Second, you may encounter criminal activity ranging from malicious hoaxes, to threats targeting specific individuals or the general public, to the purposeful exposure and infection of others with COVID-19. Because coronavirus appears to meet the statutory definition of a "biological agent" under 18 U.S.C. § 178(1), such acts potentially could implicate the Nation's terrorism-related statutes. *See, e.g.*, *id.* § 175 (development/possession of a biological agent for use as a weapon); *id.* § 875 (threats by wire); *id.* § 876 (threats by mail); *id.* § 1038 (false information and hoaxes regarding biological weapons); *id.* § 2332a (use of a weapon involving a biological agent). Threats or attempts to use COVID-19 as a weapon against Americans will not be tolerated.

Third, individuals or businesses may be accumulating medical supplies or devices beyond what they reasonably need on a daily basis, or for the purpose of selling them in excess of prevailing market prices. As discussed in a memorandum issued by the Attorney General today, it is illegal to acquire medical supplies and devices designated by the Secretary of Health and Human Services (HHS) as scarce in order to hoard them or sell them for excessive prices. Such conduct may be prosecuted under the Defense Production Act. *See* 50 U.S.C. §§ 4512, 4513.

Although no items have yet been designated, the Department will work closely with the HHS Secretary in connection with that process in the days ahead. Your Offices should coordinate with the newly constituted task force led by Craig Carpenito, the United States Attorney in the District of New Jersey, when investigating and prosecuting this conduct.

Finally, conspiracies between individuals or businesses to fix prices, rig bids, or allocate markets with respect to COVID-19 materials are prosecuted criminally under the federal antitrust laws. *See* 15 U.S.C. § 1. Monopolization or anticompetitive agreements related to critical materials needed to respond to COVID-19 can be pursued civilly under the Sherman and the Clayton Antitrust Acts. *See, e.g.*, 15 U.S.C. § 1 (anticompetitive agreements); *id.* § 2 (monopolization); *id.* § 14 (exclusive dealings). And when the United States is injured as a result of those practices, the government may bring suit to recover its damages. *See id.* § 15a (damages actions when the government is the victim).

The legal authorities set forth above are not an exhaustive list, and there may be situations where other authorities could be applied. You are encouraged to consult with either Adam Braverman or William Hughes in my office if a COVID-19-related issue warrants consideration of other authorities.

III. STATE AND LOCAL COORDINATION

While the Department of Justice is the world's premier law enforcement institution, we cannot protect the public from these schemes alone. Your Office is thus encouraged to work closely with state and local authorities to ensure both that we hear about misconduct as quickly as possible and that all appropriate enforcement tools are available to punish it.

We have also publicized a hotline for individuals to report coronavirus-related complaints – The National Center for Disaster Fraud (NCDF) Hotline – 1-866-720-5721 or disaster@leo.gov. I remind you to consult, as needed, with the Civil Division's Consumer Protection Branch (Gus Eyler), the Criminal Division's Fraud Section (John Cronan), and the Antitrust Division (Richard Powers) for additional guidance on how to detect, investigate, and prosecute these schemes.

We must do the best we can to protect Americans' rights and safety in this novel and troubling time. I thank you all for your service to this country.

Wednesday, March 18, 2020 6:34 PM
Subject: Message from the Deputy Attorney General
Importance: High

TO: ALL UNITED STATES ATTORNEYS
ALL FIRST ASSISTANT UNITED STATES ATTORNEYS
ALL EXECUTIVE ASSISTANT UNITED STATES ATTORNEYS
ALL CRIMINAL CHIEFS

RE: Continuing to Investigate and Prosecute Federal Crime

Thank you for your continuing commitment to protect the public as we adapt to the new challenges posed by the spread of coronavirus. The investigation and prosecution of crime is and remains an essential function of our government, and I am pleased to see that our federal law enforcement agents and prosecutors continue to vigilantly guard the public from those criminal actors who might try to take advantage of what they perceive to be a vulnerable time for our country.

Lest there be any doubt, the Department's law enforcement agencies, U.S. Attorneys' Offices and supporting components are and must remain active, capable and committed to advancing our mission to protect the public. No category of federal criminal investigation or prosecution has been suspended. Rather, our component heads and local leaders have been empowered to protect our workforce colleagues by using teleworking, rotating schedules and other means to assure that federal law enforcement will continue uninterrupted.

With respect to U.S. Attorneys' Offices, our prosecutors are and must remain ready to work with our law enforcement partners to advance our collective mission. Consistent with our prior guidance, local offices have availed themselves of teleworking and other strategies, where appropriate, to protect our workforce while remaining able to work closely with agents and local law enforcement. Much of our investigative work and case building can be done electronically. Indeed, much of the process that drives criminal investigations, from grand jury subpoenas to search warrants, are generated electronically and submitted to recipients via email or telephonically. These options always have been available, and may make especially good sense now, as we move forward with our cases in the current environment.

Similarly, our law enforcement agencies are and must continue to protect the public from wrongdoers. To date, our agencies have adapted to the current environment by implementing social distancing and remote work where feasible, and by taking management steps to ensure that agents are available to work proactively and also to respond to unforeseen events. Each agency is taking steps to protect its workforce based on the particular circumstances of their physical environments and the specific challenges and demands presented by their area of responsibility.

As always, we all must apply a rule of reason to protect the public and also our workforce colleagues. As we protect ourselves, we will not lose sight of our primary responsibility to protect others. Where the evidence and good judgment of our prosecutors and agents supports custodial arrests, we will not hesitate to take wrongdoers into custody. It is imperative that criminals know that this national crisis offers no safe harbor for them. We all will need to continue to adapt and to work together to ensure that those who violate federal law are brought to justice. Thank you for your commitment and your remarkable tenacity and resilience.

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated June 2020)

Introduction

The "Principles of Federal Prosecution of Business Organizations" in the Justice Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporation, determining whether to bring charges, and negotiating plea or other agreements. JM 9-28.300. These factors include "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision" and the corporation's remedial efforts "to implement an adequate and effective corporate compliance program or to improve an existing one." JM 9-28.300 (citing JM 9-28.800 and JM 9-28.1000). Additionally, the United States Sentencing Guidelines advise that consideration be given to whether the corporation had in place at the time of the misconduct an effective compliance program for purposes of calculating the appropriate organizational criminal fine. *See* U.S.S.G. §§ 8B2.1, 8C2.5(f), and 8C2.8(11). Moreover, the memorandum entitled "Selection of Monitors in Criminal Division Matters" issued by Assistant Attorney General Brian Benczkowski (hereafter, the "Benczkowski Memo") instructs prosecutors to consider, at the time of the resolution, "whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems" and "whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future" to determine whether a monitor is appropriate.

This document is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate (1) form of any resolution or prosecution; (2) monetary penalty, if any; and (3) compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations).

Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Criminal Division does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make a reasonable, individualized determination in each case that considers various factors including, but not limited to, the company's size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company's operations, that might impact its compliance program. There are, however, common questions that we may ask in the course of making an individualized determination. As the Justice Manual notes, there are three "fundamental questions" a prosecutor should ask:

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated June 2020)

1. "Is the corporation's compliance program well designed?"
2. "Is the program being applied earnestly and in good faith?" In other words, is the program adequately resourced and empowered to function effectively?
3. "Does the corporation's compliance program work" in practice?

See JM 9-28.800.

In answering each of these three "fundamental questions," prosecutors may evaluate the company's performance on various topics that the Criminal Division has frequently found relevant in evaluating a corporate compliance program both at the time of the offense and at the time of the charging decision and resolution.[1] The sample topics and questions below form neither a checklist nor a formula. In any particular case, the topics and questions set forth below may not all be relevant, and others may be more salient given the particular facts at issue and the circumstances of the company.[2] Even though we have organized the topics under these three fundamental questions, we recognize that some topics necessarily fall under more than one category.

I. Is the Corporation's Compliance Program Well Designed?

The "critical factors in evaluating any program are whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct." JM 9-28.800.

Accordingly, prosecutors should examine "the comprehensiveness of the compliance program," JM 9-28.800, ensuring that there is not only a clear message that misconduct is not tolerated, but also policies and procedures – from appropriate assignments of responsibility, to training programs, to systems of incentives and discipline – that ensure the compliance program is well-integrated into the company's operations and workforce.

A. Risk Assessment

The starting point for a prosecutor's evaluation of whether a company has a well-designed compliance program is to understand the company's business from a commercial perspective, how the company has identified, assessed, and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks. In short, prosecutors should endeavor to understand why the company has chosen to set up the compliance program the way that it has, and why and how the company's compliance program has evolved over time.

Prosecutors should consider whether the program is appropriately "designed to detect the particular types of misconduct most likely to occur in a particular corporation's line of business" and "complex regulatory environment[]." JM 9-28.800.[3] For example, prosecutors should consider whether the company has analyzed and addressed the varying risks presented by, among other factors, the location of its operations, the industry sector, the competitiveness of the market, the regulatory landscape, potential clients and business partners, transactions with foreign governments, payments to foreign officials, use of third parties, gifts, travel, and entertainment expenses, and charitable and political donations.

Prosecutors should also consider "[t]he effectiveness of the company's risk assessment and the manner in which the company's compliance program has been tailored based on that risk assessment" and whether its criteria are "periodically updated." *See, e.g.*, JM 9-47-120(2)(c); U.S.S.G. § 8B2.1(c) ("the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement [of the compliance program] to reduce the risk of criminal conduct").

Prosecutors may credit the quality and effectiveness of a risk-based compliance program that devotes appropriate attention and resources to high-risk transactions, even if it fails to prevent an infraction. Prosecutors should therefore consider, as an indicator of risk-tailoring, "revisions to corporate compliance programs in light of lessons learned." JM 9-28.800.

- **Risk Management Process** – What methodology has the company used to identify, analyze, and address the particular risks it faces? What information or metrics has the company collected and used to help detect the type of misconduct in question? How have the information or metrics informed the company's compliance program?

- **Risk-Tailored Resource Allocation –** Does the company devote a disproportionate amount of time to policing low-risk areas instead of high-risk areas, such as questionable payments to third-party consultants, suspicious trading activity, or excessive discounts to resellers and distributors? Does the company give greater scrutiny, as warranted, to high-risk transactions (for instance, a large-dollar contract with a government agency in a high-risk country) than more modest and routine hospitality and entertainment?

- **Updates and Revisions** – Is the risk assessment current and subject to periodic review? Is the periodic review limited to a "snapshot" in time or based upon continuous access to operational data and information across functions? Has the periodic review led to updates in policies, procedures, and controls? Do these updates account for risks discovered through misconduct or other problems with the compliance program?

- **Lessons Learned** – Does the company have a process for tracking and incorporating into its periodic risk assessment lessons learned either from the company's own prior issues or from those of other companies operating in the same industry and/or geographical region?

B. Policies and Procedures

Any well-designed compliance program entails policies and procedures that give both content and effect to ethical norms and that address and aim to reduce risks identified by the company as part of its risk assessment process. As a threshold matter, prosecutors should examine whether the company has a code of conduct that sets forth, among other things, the company's commitment to full compliance with relevant Federal laws that is accessible and applicable to all company employees. As a corollary, prosecutors should also assess whether the company has established policies and procedures that incorporate the culture of compliance into its day-to-day operations.

- **Design** – What is the company's process for designing and implementing new policies and procedures and updating existing policies and procedures, and has that process changed over time? Who has been involved in the design of policies and procedures? Have business units been consulted prior to rolling them out?

- **Comprehensiveness** – What efforts has the company made to monitor and implement policies and procedures that reflect and deal with the spectrum of risks it faces, including changes to the legal and regulatory landscape?

- **Accessibility** – How has the company communicated its policies and procedures to all employees and relevant third parties? If the company has foreign subsidiaries, are there linguistic or other barriers to foreign employees' access? Have the policies and procedures been published in a searchable format for easy reference? Does the company track access to various policies and procedures to understand what policies are attracting more attention from relevant employees?

- **Responsibility for Operational Integration** – Who has been responsible for integrating policies and procedures? Have they been rolled out in a way that ensures employees' understanding of the policies? In what specific ways are compliance policies and procedures reinforced through the company's internal control systems?

- **Gatekeepers** – What, if any, guidance and training has been provided to key gatekeepers in the control processes (*e.g.*, those with approval authority or

certification responsibilities)? Do they know what misconduct to look for? Do they know when and how to escalate concerns?

C. Training and Communications

Another hallmark of a well-designed compliance program is appropriately tailored training and communications.

Prosecutors should assess the steps taken by the company to ensure that policies and procedures have been integrated into the organization, including through periodic training and certification for all directors, officers, relevant employees, and, where appropriate, agents and business partners. Prosecutors should also assess whether the company has relayed information in a manner tailored to the audience's size, sophistication, or subject matter expertise. Some companies, for instance, give employees practical advice or case studies to address real-life scenarios, and/or guidance on how to obtain ethics advice on a case-by-case basis as needs arise. Other companies have invested in shorter, more targeted training sessions to enable employees to timely identify and raise issues to appropriate compliance, internal audit, or other risk management functions. Prosecutors should also assess whether the training adequately covers prior compliance incidents and how the company measures the effectiveness of its training curriculum.

Prosecutors, in short, should examine whether the compliance program is being disseminated to, and understood by, employees in practice in order to decide whether the compliance program is "truly effective." JM 9-28.800.

- **Risk-Based Training** – What training have employees in relevant control functions received? Has the company provided tailored training for high-risk and control employees, including training that addresses risks in the area where the misconduct occurred? Have supervisory employees received different or supplementary training? What analysis has the company undertaken to determine who should be trained and on what subjects?

- **Form/Content/Effectiveness of Training** – Has the training been offered in the form and language appropriate for the audience? Is the training provided online or in-person (or both), and what is the company's rationale for its choice? Has the training addressed lessons learned from prior compliance incidents? Whether online or in-person, is there a process by which employees can ask questions arising out of the trainings? How has the company measured the effectiveness of the training? Have employees been tested on what they have learned? How has the company addressed

employees who fail all or a portion of the testing? Has the company evaluated the extent to which the training has an impact on employee behavior or operations?

- **Communications about Misconduct** – What has senior management done to let employees know the company's position concerning misconduct? What communications have there been generally when an employee is terminated or otherwise disciplined for failure to comply with the company's policies, procedures, and controls (*e.g.*, anonymized descriptions of the type of misconduct that leads to discipline)?

- **Availability of Guidance** – What resources have been available to employees to provide guidance relating to compliance policies? How has the company assessed whether its employees know when to seek advice and whether they would be willing to do so?

D. Confidential Reporting Structure and Investigation Process

Another hallmark of a well-designed compliance program is the existence of an efficient and trusted mechanism by which employees can anonymously or confidentially report allegations of a breach of the company's code of conduct, company policies, or suspected or actual misconduct. Prosecutors should assess whether the company's complaint-handling process includes proactive measures to create a workplace atmosphere without fear of retaliation, appropriate processes for the submission of complaints, and processes to protect whistleblowers. Prosecutors should also assess the company's processes for handling investigations of such complaints, including the routing of complaints to proper personnel, timely completion of thorough investigations, and appropriate follow-up and discipline.

Confidential reporting mechanisms are highly probative of whether a company has "established corporate governance mechanisms that can effectively detect and prevent misconduct." JM 9-28.800; *see also* U.S.S.G. § 8B2.1(b)(5)(C) (an effectively working compliance program will have in place, and have publicized, "a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation").

- **Effectiveness of the Reporting Mechanism** – Does the company have an anonymous reporting mechanism and, if not, why not? How is the reporting mechanism publicized to the company's employees and other third parties? Has it been used? Does the company take measures to test whether employees are aware of the hotline and feel comfortable using it? How has the company assessed the seriousness of the

allegations it received? Has the compliance function had full access to reporting and investigative information?

- **Properly Scoped Investigations by Qualified Personnel** – How does the company determine which complaints or red flags merit further investigation? How does the company ensure that investigations are properly scoped? What steps does the company take to ensure investigations are independent, objective, appropriately conducted, and properly documented? How does the company determine who should conduct an investigation, and who makes that determination?

- **Investigation Response** – Does the company apply timing metrics to ensure responsiveness? Does the company have a process for monitoring the outcome of investigations and ensuring accountability for the response to any findings or recommendations?

- **Resources and Tracking of Results** – Are the reporting and investigating mechanisms sufficiently funded? How has the company collected, tracked, analyzed, and used information from its reporting mechanisms? Does the company periodically analyze the reports or investigation findings for patterns of misconduct or other red flags for compliance weaknesses? Does the company periodically test the effectiveness of the hotline, for example by tracking a report from start to finish?

E. Third Party Management

A well-designed compliance program should apply risk-based due diligence to its third-party relationships. Although the need for, and degree of, appropriate due diligence may vary based on the size and nature of the company, transaction, and third party, prosecutors should assess the extent to which the company has an understanding of the qualifications and associations of third-party partners, including the agents, consultants, and distributors that are commonly used to conceal misconduct, such as the payment of bribes to foreign officials in international business transactions.

Prosecutors should also assess whether the company knows the business rationale for needing the third party in the transaction, and the risks posed by third-party partners, including the third-party partners' reputations and relationships, if any, with foreign officials. For example, a prosecutor should analyze whether the company has ensured that contract terms with third parties specifically describe the services to be performed, that the third party is actually performing the work, and that its compensation is commensurate with the work being provided in that industry and geographical region. Prosecutors should further assess whether the

company engaged in ongoing monitoring of the third-party relationships, be it through updated due diligence, training, audits, and/or annual compliance certifications by the third party.

In sum, a company's third-party management practices are a factor that prosecutors should assess to determine whether a compliance program is in fact able to "detect the particular types of misconduct most likely to occur in a particular corporation's line of business." JM 9-28.800.

- **Risk-Based and Integrated Processes** – How has the company's third-party management process corresponded to the nature and level of the enterprise risk identified by the company? How has this process been integrated into the relevant procurement and vendor management processes?

- **Appropriate Controls** – How does the company ensure there is an appropriate business rationale for the use of third parties? If third parties were involved in the underlying misconduct, what was the business rationale for using those third parties? What mechanisms exist to ensure that the contract terms specifically describe the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered?

- **Management of Relationships** – How has the company considered and analyzed the compensation and incentive structures for third parties against compliance risks? How does the company monitor its third parties? Does the company have audit rights to analyze the books and accounts of third parties, and has the company exercised those rights in the past? How does the company train its third party relationship managers about compliance risks and how to manage them? How does the company incentivize compliance and ethical behavior by third parties? Does the company engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process?

- **Real Actions and Consequences** – Does the company track red flags that are identified from due diligence of third parties and how those red flags are addressed? Does the company keep track of third parties that do not pass the company's due diligence or that are terminated, and does the company take steps to ensure that those third parties are not hired or re-hired at a later date? If third parties were involved in the misconduct at issue in the investigation, were red flags identified from the due diligence or after hiring the third party, and how were they resolved? Has a similar third party been suspended, terminated, or audited as a result of compliance issues?

F. Mergers and Acquisitions (M&A)

A well-designed compliance program should include comprehensive due diligence of any acquisition targets, as well as a process for timely and orderly integration of the acquired entity into existing compliance program structures and internal controls. Pre-M&A due diligence, where possible, enables the acquiring company to evaluate more accurately each target's value and negotiate for the costs of any corruption or misconduct to be borne by the target. Flawed or incomplete pre- or post-acquisition due diligence and integration can allow misconduct to continue at the target company, causing resulting harm to a business's profitability and reputation and risking civil and criminal liability.

The extent to which a company subjects its acquisition targets to appropriate scrutiny is indicative of whether its compliance program is, as implemented, able to effectively enforce its internal controls and remediate misconduct at all levels of the organization.

- **Due Diligence Process** – Was the company able to complete pre-acquisition due diligence and, if not, why not? Was the misconduct or the risk of misconduct identified during due diligence? Who conducted the risk review for the acquired/merged entities and how was it done? What is the M&A due diligence process generally?

- **Integration in the M&A Process** – How has the compliance function been integrated into the merger, acquisition, and integration process?

- **Process Connecting Due Diligence to Implementation** – What has been the company's process for tracking and remediating misconduct or misconduct risks identified during the due diligence process? What has been the company's process for implementing compliance policies and procedures, and conducting post-acquisition audits, at newly acquired entities?

II. Is the Corporation's Compliance Program Adequately Resourced and Empowered to Function Effectively?

Even a well-designed compliance program may be unsuccessful in practice if implementation is lax, under-resourced, or otherwise ineffective. Prosecutors are instructed to probe specifically whether a compliance program is a "paper program" or one "implemented, reviewed, and revised, as appropriate, in an effective manner." JM 9-28.800. In addition, prosecutors should determine "whether the corporation has provided for a staff sufficient to audit, document, analyze, and utilize the results of the corporation's compliance efforts." JM 9-28.800. Prosecutors should also determine "whether the corporation's employees are adequately informed about the compliance program and are convinced of the corporation's

commitment to it." JM 9-28.800; *see also* JM 9-47.120(2)(c) (criteria for an effective compliance program include "[t]he company's culture of compliance, including awareness among employees that any criminal conduct, including the conduct underlying the investigation, will not be tolerated").

A. Commitment by Senior and Middle Management

Beyond compliance structures, policies, and procedures, it is important for a company to create and foster a culture of ethics and compliance with the law at all levels of the company. The effectiveness of a compliance program requires a high-level commitment by company leadership to implement a culture of compliance from the middle and the top.

The company's top leaders – the board of directors and executives – set the tone for the rest of the company. Prosecutors should examine the extent to which senior management have clearly articulated the company's ethical standards, conveyed and disseminated them in clear and unambiguous terms, and demonstrated rigorous adherence by example. Prosecutors should also examine how middle management, in turn, have reinforced those standards and encouraged employees to abide by them. *See* U.S.S.G. § 8B2.1(b)(2)(A)-(C) (the company's "*governing authority* shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight" of it; "[*h*]*igh-level personnel* … shall ensure that the organization has an effective compliance and ethics program" (emphasis added)).

- **Conduct at the Top** – How have senior leaders, through their words and actions, encouraged or discouraged compliance, including the type of misconduct involved in the investigation? What concrete actions have they taken to demonstrate leadership in the company's compliance and remediation efforts? How have they modelled proper behavior to subordinates? Have managers tolerated greater compliance risks in pursuit of new business or greater revenues? Have managers encouraged employees to act unethically to achieve a business objective, or impeded compliance personnel from effectively implementing their duties?

- **Shared Commitment** – What actions have senior leaders and middle-management stakeholders (*e.g.*, business and operational managers, finance, procurement, legal, human resources) taken to demonstrate their commitment to compliance or compliance personnel, including their remediation efforts? Have they persisted in that commitment in the face of competing interests or business objectives?

- **Oversight** – What compliance expertise has been available on the board of directors? Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions? What types of information have

the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?

B. Autonomy and Resources

Effective implementation also requires those charged with a compliance program's day-to-day oversight to act with adequate authority and stature. As a threshold matter, prosecutors should evaluate how the compliance program is structured. Additionally, prosecutors should address the sufficiency of the personnel and resources within the compliance function, in particular, whether those responsible for compliance have: (1) sufficient seniority within the organization; (2) sufficient resources, namely, staff to effectively undertake the requisite auditing, documentation, and analysis; and (3) sufficient autonomy from management, such as direct access to the board of directors or the board's audit committee. The sufficiency of each factor, however, will depend on the size, structure, and risk profile of the particular company. "A large organization generally shall devote more formal operations and greater resources . . . than shall a small organization." Commentary to U.S.S.G. § 8B2.1 note 2(C). By contrast, "a small organization may [rely on] less formality and fewer resources." *Id.* Regardless, if a compliance program is to be truly effective, compliance personnel must be empowered within the company.

Prosecutors should evaluate whether "internal audit functions [are] conducted at a level sufficient to ensure their independence and accuracy," as an indicator of whether compliance personnel are in fact empowered and positioned to "effectively detect and prevent misconduct." JM 9-28.800. Prosecutors should also evaluate "[t]he resources the company has dedicated to compliance," "[t]he quality and experience of the personnel involved in compliance, such that they can understand and identify the transactions and activities that pose a potential risk," and "[t]he authority and independence of the compliance function and the availability of compliance expertise to the board." JM 9-47.120(2)(c); *see also* JM 9-28.800 (instructing prosecutors to evaluate whether "the directors established an information and reporting system in the organization reasonably designed to provide management and directors with timely and accurate information sufficient to allow them to reach an informed decision regarding the organization's compliance with the law"); U.S.S.G. § 8B2.1(b)(2)(C) (those with "day-to-day operational responsibility" shall have "adequate resources, appropriate authority and direct access to the governing authority or an appropriate subgroup of the governing authority").

- **Structure** – Where within the company is the compliance function housed (e.g., within the legal department, under a business function, or as an independent function reporting to the CEO and/or board)? To whom does the compliance function report? Is the compliance function run by a designated chief compliance officer, or another executive within the company, and does that person have other roles within the company? Are compliance personnel dedicated to compliance responsibilities, or do

they have other, non-compliance responsibilities within the company? Why has the company chosen the compliance structure it has in place? What are the reasons for the structural choices the company has made?

- **Seniority and Stature** – How does the compliance function compare with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers? What has been the turnover rate for compliance and relevant control function personnel? What role has compliance played in the company's strategic and operational decisions? How has the company responded to specific instances where compliance raised concerns? Have there been transactions or deals that were stopped, modified, or further scrutinized as a result of compliance concerns?

- **Experience and Qualifications** – Do compliance and control personnel have the appropriate experience and qualifications for their roles and responsibilities? Has the level of experience and qualifications in these roles changed over time? How does the company invest in further training and development of the compliance and other control personnel? Who reviews the performance of the compliance function and what is the review process?

- **Funding and Resources** – Has there been sufficient staffing for compliance personnel to effectively audit, document, analyze, and act on the results of the compliance efforts? Has the company allocated sufficient funds for the same? Have there been times when requests for resources by compliance and control functions have been denied, and if so, on what grounds?

- **Data Resources and Access** – Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions? Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?

- **Autonomy** – Do the compliance and relevant control functions have direct reporting lines to anyone on the board of directors and/or audit committee? How often do they meet with directors? Are members of the senior management present for these meetings? How does the company ensure the independence of the compliance and control personnel?

- **Outsourced Compliance Functions** – Has the company outsourced all or parts of its compliance functions to an external firm or consultant? If so, why, and who is responsible for overseeing or liaising with the external firm or consultant? What level of access does the external firm or consultant have to company information? How has the effectiveness of the outsourced process been assessed?

C. Incentives and Disciplinary Measures

Another hallmark of effective implementation of a compliance program is the establishment of incentives for compliance and disincentives for non-compliance. Prosecutors should assess whether the company has clear disciplinary procedures in place, enforces them consistently across the organization, and ensures that the procedures are commensurate with the violations. Prosecutors should also assess the extent to which the company's communications convey to its employees that unethical conduct will not be tolerated and will bring swift consequences, regardless of the position or title of the employee who engages in the conduct. *See* U.S.S.G. § 8B2.1(b)(5)(C) ("the organization's compliance program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct").

By way of example, some companies have found that publicizing disciplinary actions internally, where appropriate and possible, can have valuable deterrent effects. At the same time, some companies have also found that providing positive incentives – personnel promotions, rewards, and bonuses for improving and developing a compliance program or demonstrating ethical leadership – have driven compliance. Some companies have even made compliance a significant metric for management bonuses and/or have made working on compliance a means of career advancement.

- **Human Resources Process** – Who participates in making disciplinary decisions, including for the type of misconduct at issue? Is the same process followed for each instance of misconduct, and if not, why? Are the actual reasons for discipline communicated to employees? If not, why not? Are there legal or investigation-related reasons for restricting information, or have pre-textual reasons been provided to protect the company from whistleblowing or outside scrutiny?

- **Consistent Application** – Have disciplinary actions and incentives been fairly and consistently applied across the organization? Does the compliance function monitor its investigations and resulting discipline to ensure consistency? Are there similar instances of misconduct that were treated disparately, and if so, why?

- **Incentive System** – Has the company considered the implications of its incentives and rewards on compliance? How does the company incentivize compliance and ethical behavior? Have there been specific examples of actions taken (*e.g.*, promotions or awards denied) as a result of compliance and ethics considerations? Who determines the compensation, including bonuses, as well as discipline and promotion of compliance personnel?

III. Does the Corporation's Compliance Program Work in Practice?

The Principles of Federal Prosecution of Business Organizations require prosecutors to assess "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision." JM 9-28.300. Due to the backward-looking nature of the first inquiry, one of the most difficult questions prosecutors must answer in evaluating a compliance program following misconduct is whether the program was working effectively at the time of the offense, especially where the misconduct was not immediately detected.

In answering this question, it is important to note that the existence of misconduct does not, by itself, mean that a compliance program did not work or was ineffective at the time of the offense. *See* U.S.S.G. § 8B2.1(a) ("[t]he failure to prevent or detect the instant offense does not mean that the program is not generally effective in preventing and deterring misconduct"). Indeed, "[t]he Department recognizes that no compliance program can ever prevent all criminal activity by a corporation's employees." JM 9-28.800. Of course, if 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.

In assessing whether a company's compliance program was effective at the time of the misconduct, prosecutors should consider whether and how the misconduct was detected, what investigation resources were in place to investigate suspected misconduct, and the nature and thoroughness of the company's remedial efforts.

To determine whether a company's compliance program is working effectively at the time of a charging decision or resolution, prosecutors should consider whether the program evolved over time to address existing and changing compliance risks. Prosecutors should also consider whether the company undertook an adequate and honest root cause analysis to understand both what contributed to the misconduct and the degree of remediation needed to prevent similar events in the future.

For example, prosecutors should consider, among other factors, "whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems" and "whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future." Benczkowski Memo at 2 (observing that "[w]here a corporation's compliance program and controls are demonstrated to be effective and appropriately resourced at the time of resolution, a monitor will not likely be necessary").

A. Continuous Improvement, Periodic Testing, and Review

One hallmark of an effective compliance program is its capacity to improve and evolve. The actual implementation of controls in practice will necessarily reveal areas of risk and potential adjustment. A company's business changes over time, as do the environments in which it operates, the nature of its customers, the laws that govern its actions, and the applicable industry standards. Accordingly, prosecutors should consider whether the company has engaged in meaningful efforts to review its compliance program and ensure that it is not stale. Some companies survey employees to gauge the compliance culture and evaluate the strength of controls, and/or conduct periodic audits to ensure that controls are functioning well, though the nature and frequency of evaluations may depend on the company's size and complexity.

Prosecutors may reward efforts to promote improvement and sustainability. In evaluating whether a particular compliance program works in practice, prosecutors should consider "revisions to corporate compliance programs in light of lessons learned." JM 9-28.800; *see also* JM 9-47-120(2)(c) (looking to "[t]he auditing of the compliance program to assure its effectiveness"). Prosecutors should likewise look to whether a company has taken "reasonable steps" to "ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct," and "evaluate periodically the effectiveness of the organization's" program. U.S.S.G. § 8B2.1(b)(5). Proactive efforts like these may not only be rewarded in connection with the form of any resolution or prosecution (such as through remediation credit or a lower applicable fine range under the Sentencing Guidelines), but more importantly, may avert problems down the line.

- **Internal Audit** – What is the process for determining where and how frequently internal audit will undertake an audit, and what is the rationale behind that process? How are audits carried out? What types of audits would have identified issues relevant to the misconduct? Did those audits occur and what were the findings? What types of relevant audit findings and remediation progress have been reported to management and the board on a regular basis? How have management and the board followed up? How often does internal audit conduct assessments in high-risk areas?

- **Control Testing** – Has the company reviewed and audited its compliance program in the area relating to the misconduct? More generally, what testing of controls, collection and analysis of compliance data, and interviews of employees and third parties does the company undertake? How are the results reported and action items tracked?

- **Evolving Updates** – How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices? Has the company undertaken a gap analysis to determine if particular areas of risk are not sufficiently addressed in its policies, controls, or training? What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries? Does the company review and adapt its compliance program based upon lessons learned from its own misconduct and/or that of other companies facing similar risks?

- **Culture of Compliance** – How often and how does the company measure its culture of compliance? Does the company seek input from all levels of employees to determine whether they perceive senior and middle management's commitment to compliance? What steps has the company taken in response to its measurement of the compliance culture?

B. Investigation of Misconduct

Another hallmark of a compliance program that is working effectively is the existence of a well-functioning and appropriately funded mechanism for the timely and thorough investigations of any allegations or suspicions of misconduct by the company, its employees, or agents. An effective investigations structure will also have an established means of documenting the company's response, including any disciplinary or remediation measures taken.

- **Properly Scoped Investigation by Qualified Personnel** – How has the company ensured that the investigations have been properly scoped, and were independent, objective, appropriately conducted, and properly documented?

- **Response to Investigations** – Have the company's investigations been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory managers and senior executives? What has been the process for responding to investigative findings? How high up in the company do investigative findings go?

C. Analysis and Remediation of Any Underlying Misconduct

Finally, a hallmark of a compliance program that is working effectively in practice is the extent to which a company is able to conduct a thoughtful root cause analysis of misconduct and timely and appropriately remediate to address the root causes.

Prosecutors evaluating the effectiveness of a compliance program are instructed to reflect back on "the extent and pervasiveness of the criminal misconduct; the number and level of the corporate employees involved; the seriousness, duration, and frequency of the misconduct; and any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program, and revisions to corporate compliance programs in light of lessons learned." JM 9-28.800; *see also* JM 9-47.120(3)(c) ("to receive full credit for timely and appropriate remediation" under the FCPA Corporate Enforcement Policy, a company should demonstrate "a root cause analysis" and, where appropriate, "remediation to address the root causes").

Prosecutors should consider "any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program." JM 98-28.800; *see also* JM 9-47-120(2)(c) (looking to "[a]ppropriate discipline of employees, including those identified by the company as responsible for the misconduct, either through direct participation or failure in oversight, as well as those with supervisory authority over the area in which the criminal conduct occurred" and "any additional steps that demonstrate recognition of the seriousness of the misconduct, acceptance of responsibility for it, and the implementation of measures to reduce the risk of repetition of such misconduct, including measures to identify future risk").

- **Root Cause Analysis** – What is the company's root cause analysis of the misconduct at issue? Were any systemic issues identified? Who in the company was involved in making the analysis?

- **Prior Weaknesses** – What controls failed? If policies or procedures should have prohibited the misconduct, were they effectively implemented, and have functions that had ownership of these policies and procedures been held accountable?

- **Payment Systems** – How was the misconduct in question funded (*e.g.*, purchase orders, employee reimbursements, discounts, petty cash)? What processes could have prevented or detected improper access to these funds? Have those processes been improved?

- **Vendor Management** – If vendors were involved in the misconduct, what was the process for vendor selection and did the vendor undergo that process?

- **Prior Indications** – Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations? What is the company's analysis of why such opportunities were missed?

- **Remediation** – What specific changes has the company made to reduce the risk that the same or similar issues will not occur in the future? What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?

- **Accountability** – What disciplinary actions did the company take in response to the misconduct and were they timely? Were managers held accountable for misconduct that occurred under their supervision? Did the company consider disciplinary actions for failures in supervision? What is the company's record (*e.g.*, number and types of disciplinary actions) on employee discipline relating to the types of conduct at issue? Has the company ever terminated or otherwise disciplined anyone (reduced or eliminated bonuses, issued a warning letter, etc.) for the type of misconduct at issue?

---

[1] Many of the topics also appear in the following resources:

- Justice Manual ("JM")
  - JM 9-28.000 Principles of Federal Prosecution of Business Organizations, Justice Manual ("JM"), *available at* https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations.
  - JM 9-47.120 FCPA Corporate Enforcement Policy, *available at* https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#9-47.120.
- Chapter 8 – Sentencing of Organizations - United States Sentencing Guidelines ("U.S.S.G."), *available at* https://www.ussc.gov/guidelines/2018-guidelines-manual/2018-chapter-8#NaN.

- Memorandum entitled "Selection of Monitors in Criminal Division Matters," issued by Assistant Attorney General Brian Benczkowski on October 11, 2018, *available at* https://www.justice.gov/criminal-fraud/file/1100366/download.

- Criminal Division corporate resolution agreements, *available at* https://www.justice.gov/news (the Department of Justice's ("DOJ") Public Affairs website contains press releases for all Criminal Division corporate resolutions which contain links to charging documents and agreements).

- A Resource Guide to the U.S. Foreign Corrupt Practices Act ("FCPA Guide"), published in November 2012 by the DOJ and the Securities and Exchange Commission ("SEC"), *available at* https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf.

- Good Practice Guidance on Internal Controls, Ethics, and Compliance, adopted by the Organization for Economic Co-operation and Development ("OECD") Council on February 18, 2010, *available at* https://www.oecd.org/daf/anti-bribery/44884389.pdf.

- Anti-Corruption Ethics and Compliance Handbook for Business ("OECD Handbook"), published in 2013 by OECD, United Nations Office on Drugs and Crime, and the World Bank, *available at* https://www.oecd.org/corruption/Anti-CorruptionEthicsComplianceHandbook.pdf.

- Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, published in July 2019 by DOJ's Antitrust Division, *available at* https://www.justice.gov/atr/page/file/1182001/download.

- A Framework for OFAC Compliance Commitments, published in May 2019 by the Department of the Treasury's Office of Foreign Assets Control ("OFAC"), *available at https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf.*

[2] Prosecutors should consider whether certain aspects of a compliance program may be impacted by foreign law. Where a company asserts that it has structured its compliance program in a particular way or has made a compliance decision based on requirements of foreign law, prosecutors should ask the company the basis for the company's conclusion about foreign law, and how the company has addressed the issue to maintain the integrity and effectiveness of its compliance program while still abiding by foreign law.

[3] As discussed in the Justice Manual, many companies operate in complex regulatory environments outside the normal experience of criminal prosecutors. JM 9-28.000. For example, financial institutions such as banks, subject to the Bank Secrecy Act statute and regulations,

require prosecutors to conduct specialized analyses of their compliance programs in the context of their anti-money laundering requirements. Consultation with the Money Laundering and Asset Recovery Section is recommended when reviewing AML compliance. *See* https://www.justice.gov/criminal-mlars. Prosecutors may also wish to review guidance published by relevant federal and state agencies. *See* Federal Financial Institutions Examination Council/Bank Secrecy Act/Anti-Money Laundering Examination Manual, *available at* https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm).