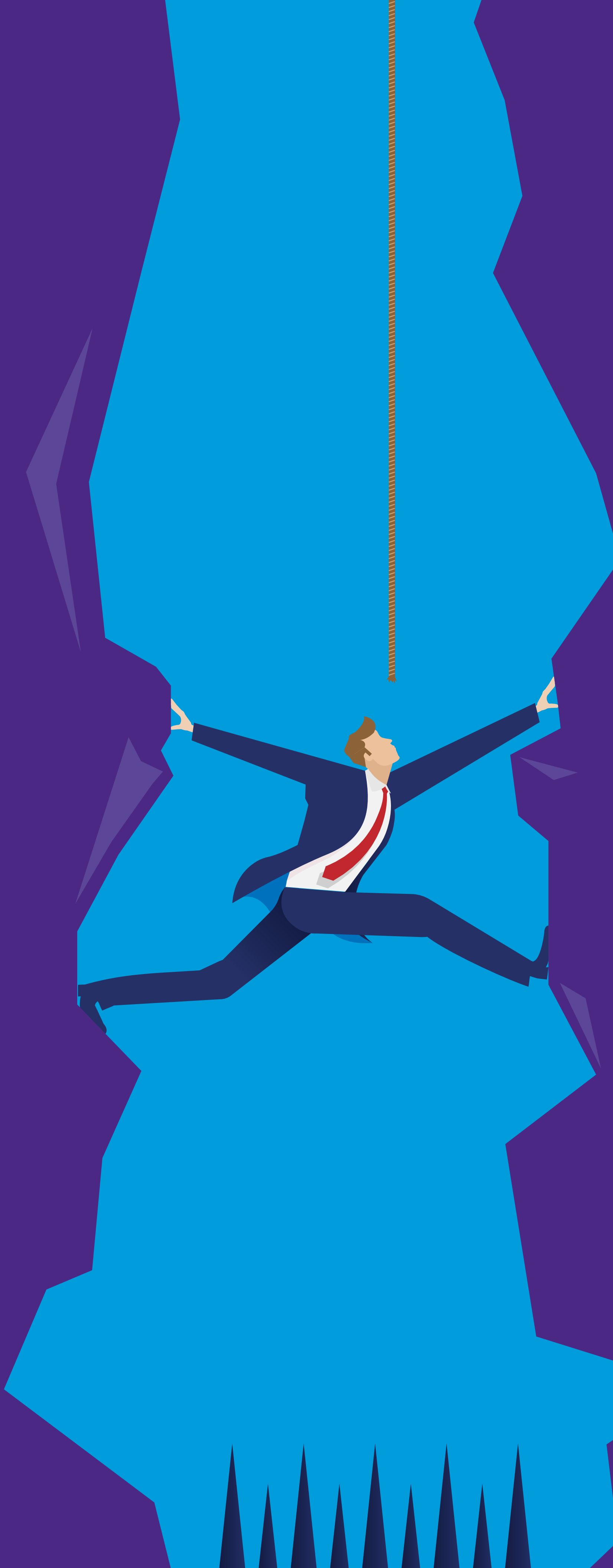
Integrity in adversity:

Raising the standard of corporate behavior in times of uncertainty

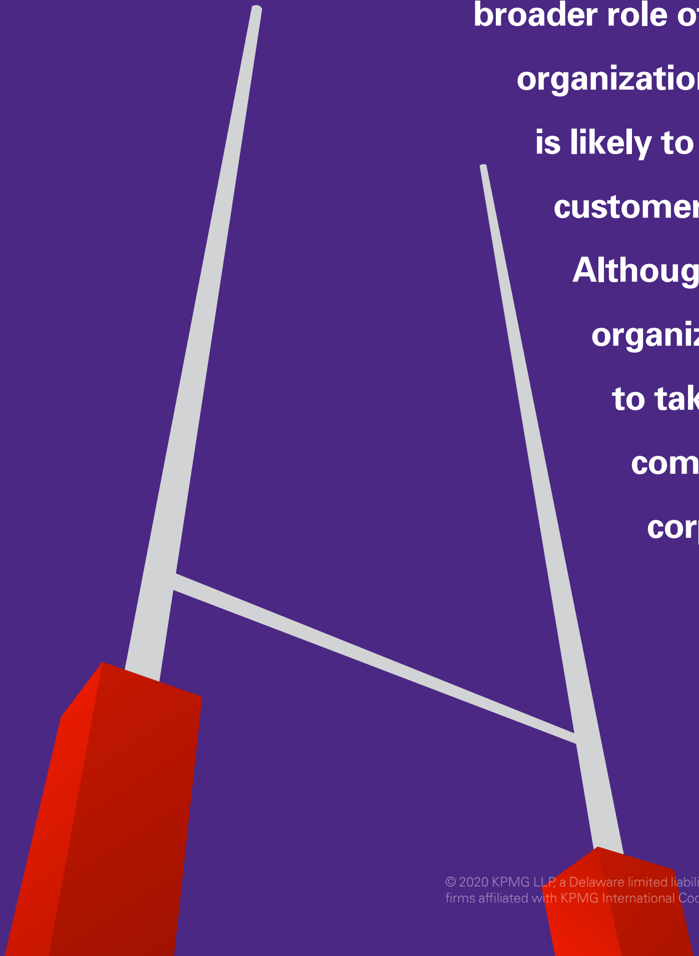


kpmg.com/us/forensic

Lifting the bar

Contents:

During periods of turmoil and uncertainty such as these, corporate integrity is more important than ever. This may seem counterintuitive, at a time when organizations and their employees face extraordinary challenges to their health and well-being, which are very basic things to worry about. However, as strange as this may seem, this murky environment is precisely when organizations should aim to raise the bar for corporate conduct. At a time of renewed concerns about the broader role of companies in society, organizations' reputation for integrity is likely to grow among regulators, customers, and employees. Although this is an uphill task, organizations should strive to take a methodical and comprehensive approach to corporate integrity.



Caught off guard

There is a strong business case to be made for a concerted push to raise the standard of corporate behavior. The risks of malfeasance and illegality are even greater now, because fraudsters and other types of criminals see the economic disarray as an opportunity to commit wrongdoing. In March 2020, for example, just as COVID-19 was spreading in the U.S., the Department of Health and Human Services confirmed it was hit by a cyberattack, after it "became aware of a significant increase in activity in HHS cyber infrastructure a day earlier that appeared to be part of a campaign of disruption and disinformation."[1]

Opportunities for fraud are likely to grow as a result of trillions of dollars of public money being allocated to rescue small and large businesses. Organizations are liable to let their guard down, as they grapple with employee and customer health issues due to the coronavirus epidemic and a suddenly weak global economy. Millions of employees are working from home, making it more difficult to secure computer networks and increasing the possibility of fraud. Companies may need to respond quickly to such things as sudden supply-chain disruptions and enlist new third-party vendors without properly vetting them. The Association of Certified Fraud Examiners (ACFE) has said, "History shows that fraudsters exploit calamity. We saw it happen in the aftermath of the 2008 financial crisis, and all signs indicate it will happen again. According to [an April 2020] survey of anti-fraud professionals, businesses are already seeing a steep rise in scams related to COVID-19."[2]

There are fewer financial and human resources available to monitor and safeguard high standards of behavior. Many organizations may not have the funds to invest in new technology to mitigate the risks of fraud, waste, abuse, or other kinds of wrongdoing. At the same time, economic distress can motivate current or former employees to commit misconduct. Often, they work with third parties, criminal organizations, or their colleagues to engage in wrongdoing. Although this report focuses primarily on internal misconduct, it should be noted that organizational walls are porous, and the line between inside and outside wrongdoing, such as the bribery of public officials, is often negligible.

[1] Source: "US health department targeted in cyber attack", *Financial Times,* Hannah Murphy and Kiran Stacey (March 16, 2020)

[2] Source: Fraud in the wake of COVID-19: Benchmarking report, Association of Certified Fraud Examiners [undated]

Malfeasance takes many forms

In order to tackle the problem of misconduct, organizations must assess the risks by analyzing the types of misconduct they might experience. These cover a wide array of illicit behavior, both fraudulent and otherwise, that could damage reputations, cause financial harm, disrupt operations, and create disarray among employees, customers, suppliers, and business partners. This could also include behavior that contravenes government regulations, such as anti-money-laundering rules, and leads to large fines or being disbarred from doing business.

Fraud comes in three categories:

1) Bribery and corruption

2) Asset misappropriation

3) Financial statement fraud

Such activities range from corruptly fixing the bidding for a public works contract, to fraudulently overstating expenses for reimbursement, or falsifying the true value of a company. When all these elements are added together, the total cost of fraud is enormous. The UN estimates that "every year $1 trillion is paid in bribes while an estimated $2.6 trillion are stolen annually through corruption – a sum equivalent to more than 5 per cent of the global GDP."[3]

These forms of fraud are varied, but they do not paint a complete picture of the threat landscape. There are a lot of other types of misconduct that can be as damaging as fraud. These non-fraudulent forms of misconduct tend to undermine the trust placed in employees and executives by the following:

- **Customers and market operators** (e.g., falsifying car emissions data)
- **Shareholders** (e.g., trading securities based on inside information)
- **Suppliers** (e.g., violating contract or payment terms)
- **The organization's employees** (e.g., engaging in sexual harassment)
- **Regulators, the public, and the media** (e.g., providing misleading information).

[3] Source: United against corruption for peace, development and security, United Nations (December 9, 2019)

Rhetoric and reality

Many companies espouse values of integrity and honesty, but how many live up to these ideals? KPMG LLP (KPMG) has conducted five large-scale surveys of U.S. employees at all levels of an organization since 2000 and has found consistently high levels of corporate misconduct. In the most recent of KPMG's integrity surveys, of 2,300 people, 76 percent reported that they had personally observed misconduct in the previous year. Almost as high a proportion (68 percent) said that the misconduct they observed could cause a "significant loss of public trust if discovered."

The study found that most misconduct is due to internal pressure on employees to commit wrongdoing and weak controls on corporate behavior. Sixty-five percent of survey respondents said that employees felt pressure to do "whatever it takes" to meet business targets, and almost as many (62 percent) believed that their organization's code of conduct was not taken seriously. Further, employees are not reporting misconduct often enough. Sixty-nine percent of survey respondents said that if they observed misconduct, they would try to resolve the matter directly rather than notify their supervisor or other manager.

The survey was conducted before COVID-19 struck. If evidence of wrongdoing has increased since the onset of COVID-19, as found by the ACFE, this implies that companies should not aim simply to restore the status quo before the virus, because this is too low of a bar. The upheavals of 2020 should be seen as an opportunity to set their houses in order and raise the bar higher for corporate integrity.

Benefits of a comprehensive integrity program

Corporate misconduct can harm not only internal stakeholders but also suppliers, business partners and shareholders. Only a rigorous integrity and compliance program that covers all forms of corporate misbehavior, inside and out, is likely to protect an organization's reputation.

What would such a program look like? The table here illustrates 10 elements that would comprise a comprehensive approach to corporate integrity and compliance.

Elements of an integrity and compliance program

1. A code of conduct that articulates the values and standards of the organization.
2. A senior-level ethics or compliance officer.
3. Background investigations on prospective employees.
4. Due diligence of business third parties.
5. Training about, and communication of, its code of conduct.
6. Monitors and audits employee compliance with its code of conduct.
7. Confidential and anonymous hotline for reporting misconduct or providing advice.
8. Policies to hold employees and managers accountable for code of conduct violations.
9. Incentives for staff to uphold the code of conduct.
10. Policies to investigate and take corrective action if misconduct is alleged.

KPMG's most recent survey shows that companies whose integrity programs contain all 10 elements of an integrity program tend to perceive misconduct very differently from those without such a program. This is because they understand the importance of such a holistic approach and know that if there is a weakness in any area or an absence of any elements, bad behavior is likely to crop up and may even undermine the entire edifice.

This is borne out by the survey data when comparing the views of the 24 percent of respondents who said their organization's program was comprehensive with the views of the other 76 percent of respondents who felt that their organization lacked a comprehensive program. The respondents whose organizations have a comprehensive compliance program felt much more certain that the results of an investigation into misconduct would be dealt with correctly, as can be seen in the chart. Respondents also perceived organizational leaders differently if their companies had a comprehensive compliance program: those working at organizations with comprehensive integrity programs were almost twice as likely to believe that the top executives set the right tone at the top, and roughly the same ratio feel motivated and empowered to 'do the right thing.'

Organizations with and without a comprehensive integrity and compliance program

	With comprehensive program	Without comprehensive program
Believe appropriate action would be taken if they reported misconduct	**93%**	**49%**
Believe they would be doing the right thing if they reported it	**96%**	**57%**
Believe CEO and other senior executives know what type of behavior goes on in the organization	**85%**	**44%**
Say that willingness to tolerate misconduct is minimal	**96%**	**57%**

Source: KPMG

Effective measures to deal with misconduct

These differences show that there is a wide gap in perception between those organizations that take a comprehensive approach to integrity and compliance and others that are not as meticulous. Indeed, the gap is so wide that it suggests a major cultural shift takes place when companies embark on a program to raise the bar of business conduct. To achieve this, however, is not easy; indeed, at times of adversity, as today, it may seem harder to affect change than in more normal circumstances. But when organizations are being forced to test their assumptions and consider their core values, there is an opportunity to take a fresh approach to the problem of raising standards of conduct.

It takes teamwork and tenacity to develop an organizational culture that has a high level of integrity. And it begins at the top, where leaders will have to consider whether the company's controls around prevention, detection and response to misconduct are fit for purpose. To enhance the discussion among executives regarding the effectiveness of controls, they might consider the following emerging challenges:

Prevention

The organization can begin by designing the integrity program to focus on the pressures, rationalizations, and opportunities faced by employees who engage in misconduct. The U.S. Department of Justice offers detailed guidance on the design and evaluation of such a program (see graphic on page 7). Case studies can be used to educate employees and managers on business risks they may face and the ethics and values that should inform their actions when dilemmas arise. This is as important when employees work with third parties abroad, by ensuring there is an appropriate level of due diligence on these third parties prior to entering into business relationships. Employee performance should be evaluated in a manner that properly weighs the business results against the methods used. Employees due for promotion to positions of authority should be very carefully evaluated by gathering the necessary insights into their business behavior.

Training is important, too. To mitigate the threat of a cyberattack, for example, all employees need to understand the possible ways the organization’s network might be compromised and be educated on how to prevent this from happening. They should be kept informed of new scams that might appear on the organization’s radar and reminded of the vulnerability to the types of threat that have been present for many years and are still active.

The leadership of the organization must critically examine the controls in place to prevent fraud and misconduct. The controls should be based on an assessment of the types of risk of malfeasance that are likely to arise. They should be designed in a manner consistent with legal and regulatory criteria and implemented by functions with the required levels of objectivity, competence, authority, and resources. And the controls must be regularly evaluated to ensure they are working effectively.

Detection

Technology plays an important role in measuring, monitoring, and flagging unusual transactions and business behavior. Fraud analytics and machine learning, for example, can provide useful data to decision makers and process owners, who can then judge whether an event, transaction, business proposal, or contract contains unusual features that should be investigated. The amount of information to analyze is often so large that only powerful computer programs can do the job. But to produce actionable intelligence requires considerable human skills to fine-tune the system of alerts so that compliance teams are not overwhelmed with false positives nor dulled by too many false negatives into thinking that fraud controls are working perfectly.

Analytics is only one method of detection. On the non-technological side, whistle-blower hotlines must not only be kept independent of reporting lines in the rest of the organization but must also be seen to be independent if employees are to feel confident in communicating their suspicions without fear of reprisal. Managers should also make effective use of feedback received from customer complaints and employee exit interviews and ensure that concerns raised through channels outside of whistle-blower hotlines reach the right people.

US Department of Justice guidance on effective compliance programs

Is the program well-designed?

– Risk assessments should be used to tailor the compliance program.

– Policies and procedures should be published in a searchable format.

– Training programs should help employees identify and raise compliance issues.

– Confidential reporting to hotlines should be tested for effectiveness.

– Third-party risk needs to be continually evaluated.

– Due diligence of acquisition targets should be comprehensive before and after the deal.

Is the program adequately resourced and empowered to be effective?

– A culture of ethics and compliance should exist at all levels of the organization.

– Compliance staff should have sufficient access to relevant sources of data to allow for effective monitoring.

– The compliance function should monitor investigations and disciplinary measures to ensure consistent enforcement.

Does the program work?

– Organizations should strive for continuous improvement, periodic testing, and review.

– Lessons learned from misconduct cases should be integrated into the program.

Source: Evaluation of Corporate Compliance Programs, US Department of Justice (June 2020)

Response

When wrongdoing is found, the response of the organization should be swift and rigorous. Front-line supervisors need to be trained and armed with the right tools to address allegations about misconduct. There should be a uniformly deep understanding throughout the company of what allegations require investigation, by whom, when, and in what manner. The organization requires careful guidelines on whether and how managers are held accountable for wrongdoing by subordinates. The guidelines should be formalized in documents that identify who has the authority and responsibility for handling each type of misconduct.

Oversight and evaluation

In addition to these three elements, boards of directors must be involved in setting a timetable for audit and compensation committees to discuss how to address fraud and misconduct risks. When the strategic goals of the company are established or changed, the board should ensure they align with the aims of the integrity and compliance program, while providing the stewards of the program with the appropriate level of authority to carry out their work.

The leaders of the organization will not know whether the program is effective unless they decide how to measure it. For example, should employee attitudes be included as a metric? What measurements should be shared with middle managers and employees to foster confidence in the integrity program? Should information on good governance be communicated to outside stakeholders and, if so, what? When evaluating the success, or otherwise, of the program, it should be measured not just in terms of the avoidance of risk but the benefit to the brand and the bottom line.

Creating a culture of integrity

Perhaps the most important concept that underlines the entire integrity program is holding everybody in the organization accountable for their conduct, both in their actions and in their lack of action, such as turning a blind eye to malfeasance. The program should be comprehensive in what it covers and in whom it covers. This entails:

- Recognizing that high standards of corporate conduct are not the responsibility of a few employees in the legal and compliance function but of everybody.
- Ensuring that the same rules apply equally to senior executives as to those on the lower rungs.
- Providing everybody with the right tools and processes to protect themselves and their organization from harm, whether it be the threat of fraudulent behavior, waste and abuse, or other types of corporate misconduct.

Staying risk-aware

By creating a culture of integrity during a virus outbreak and steep recession, when conditions are at their most challenging, organizations will be in a strong position to continue this work when the economic and social environment improves. Good behavior is a continuous process, not a one-off project. When the economy recovers, companies must ensure the integrity program does not finish at that point, but adapts to the changing environment. The challenges will be different when business is healthy again. The price of integrity, like freedom, is eternal vigilance.

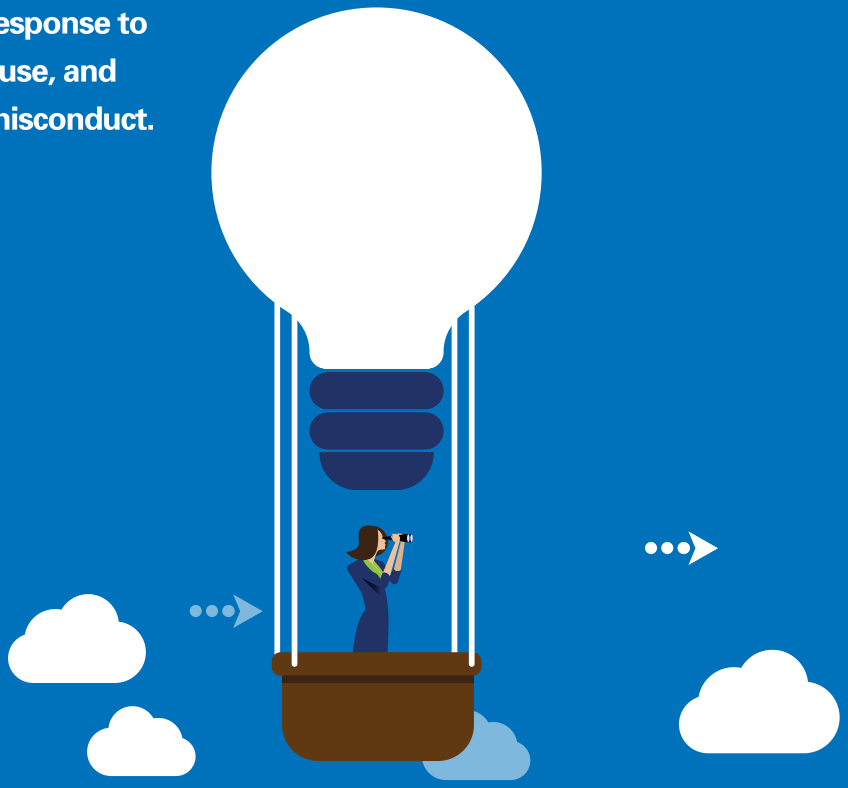
About KPMG Forensic

Enhanced by technology and infused with real-world insight, KPMG Forensic professionals transform how clients identify, mitigate, and respond to risk, saving time and money. We assist businesses to effectively manage the costs and risks of complying with new regulations and enforcement activity. We help assess, design, and implement internal controls and compliance programs to mitigate vulnerabilities to fraud and misconduct and assist in the prevention, detection, and response to fraud, waste, abuse, and other forms of misconduct.

We understand that helping clients meet their business challenges, manage risk, and navigate the dangers of costly and disruptive litigation and investigations begins with an in-depth understanding of the industries in which they work. We bring together the right industry experience to better meet the distinct needs of our clients and deliver real results.

KPMG provides access to deep forensic capabilities around the world. Our global network consists of over 3,500 multidisciplinary professionals who reside in more than 100 countries. Our professionals not only help clients discover the facts underlying concerns about fraud and misconduct but also assist clients in assessing and mitigating the vulnerabilities to such activities. We deliver a broad range of services to help prevent and resolve commercial disputes, including the assessment of damages; the resolutions of accounting, audit, and finance-related issues; and expert witness services.

Using a wide range of sophisticated technology tools, KPMG Forensic also helps organizations address the risks and costs involved with evidence and discovery management. Our professionals work alongside clients to handle information from the time of its creation to its preservation, collection, analysis, and presentation in discovery. We also apply data analytics to assist with detecting fraud and misconduct.



Contact us

Amanda Rigby

Principal, Forensic Services Leader, KPMG LLP
T: 312-665-1953 | E: amandarigby@kpmg.com

Amanda is the national services leader for KPMG Forensic. Amanda has extensive experience in the areas of investigations, regulatory compliance, and dispute advisory services. Amanda has conducted numerous financial investigations that have included allegations of earnings management, misappropriation of assets, conflicts of interest, and other noncompliance in industries such as healthcare, life sciences, consumer products, industrial manufacturing, not-for-profit, and technology. She also provides comprehensive support for clients in areas related to regulatory compliance, compliance with corporate policies, standards of acceptable behavior, and third-party risk management.

Matthew McFillin

Partner, Forensic Services, KPMG LLP
T: 267-256-2647 | E: mmcfillin@kpmg.com

Matt leads the Investigations, Disputes and Compliance solution within the KPMG Forensic practice. He provides investigative and dispute services for attorneys and corporate management on a variety of matters involving financial statement fraud investigations, Foreign Corrupt Practices Act (FCPA) concerns, government contracts, and business disputes. Matt has been involved in several matters which required him to present to and assist the United States Securities Exchange Commission (SEC), the United States Postal Inspectors, and the United States Attorney's Office.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates and related entities.

This document does not constitute or include and should not be construed to constitute or include the provision by KPMG LLP of legal advice or legal services. KPMG does not provide legal advice or legal services. All questions concerning legal interpretation or the application of law or regulations to specific facts and circumstances should be referred to legal counsel.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

kpmg.com/socialmedia