GIR INSIGHT

AMERICAS
INVESTIGATIONS REVIEW
2021

AMERICAS
INVESTIGATIONS REVIEW 2021

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2020
For further information please contact Natalie.Clarke@lbresearch.com

Published in the United Kingdom
by Global Investigations Review
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL

www.globalinvestigationsreview.com

To subscribe please contact subscriptions@globalinvestigationsreview.com

ISBN 978-1-83862-267-1

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

Contents

Cross-border overviews

Enforcer overview

Country chapters

Preface

Welcome to the *Americas Investigations Review 2020*, one of *Global Investigations Review*'s special reports. *Global Investigations Review*, for newcomers, is the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing. We tell them all they need to know about everything that matters, wherever it took place.

Throughout the year, *GIR* writes daily news, surveys and features; organises the liveliest events ('GIR Live'); and provides our readers with innovative tools; and know-how products to make life more efficient.

In addition, assisted by external contributors, we curate a range of comprehensive regional reviews – online and in print – that go deeper into developments than the exigencies of journalism allow.

The *Americas Investigations Review 2020*, which you are reading, is one of those reviews. It contains insight and thought leadership, from 28 pre-eminent practitioners from the region. Across 11 chapters, and 160 pages, it is part invaluable retrospective and part primer. All contributors are vetted for their standing and knowledge before being invited to take part.

Together, these writers capture and interpret the most substantial recent international investigations developments of the past year, with footnotes and relevant statistics. Other articles provide valuable background so that you can get up to speed quickly on the essentials of a particular topic.

This edition covers Brazil, Mexico and the United States – each from multiple perspectives, and has overviews on the Department of Justice's use of tools that are not the Foreign Corrupt Practices Act; on evidence gathering; and on how to ensure that history does not repeat – the art of learning the right lessons as an investigation winds down.

Among the highlights for this reader:

- a fine discussion of the *Bogucki* case – in which the US Department of Justice has been accused (by a former member of staff) of misusing mutual legal assistance treaty requests to stop the clock on cases;
- news that Airbus's huge settlement led to raids for other companies – notably Avianca;
- finding a worked example of how to learn the lessons at the end of an investigation (featuring hypothetical company 'ZYX Inc');

- the full breakdown of all corruption related fines and settlements levied in Brazil, complete with graphics; and
- discovering that covid-related corruption is already under investigation in Germany, Italy Serbia and Brazil, and that the new head of Mexico's Federal General Prosecutor's office is over 80 years old (and was chosen for his venerableness in part).

And much, much more.

If you have any suggestions for future editions, or want to take part in this annual project, we would love to hear from you. Please write to insight@globalarbitrationreview.com.

David Samuels
Publisher, Global Investigations Review
London
September 2020

Moving Forward after an Investigation

Frances McLeod, Jenna Voss and Umair Nadeem
Forensic Risk Alliance

In summary

We provide practical suggestions for ensuring a strong control environment post-investigation and suggest best practices that companies should consider to ensure they are well-positioned to detect and investigate future fraudulent or non-compliant behaviour. We also highlight how companies need to consider the unique challenges the covid-19 pandemic presents.

Discussion points

- Covid-19 may have limited some companies' opportunity to, or prioritisation of, conducting effective root cause analysis or risk assessments
- Economic downturns may increase an organisation's exposure to fraud and misconduct, and short-term cost savings eventually create gaps within the overall compliance programme, which can result in investigations
- Companies should not take the approach that the current business environment is only 'temporary' and should ensure effective remediation of all identified vulnerabilities
- Recent international public scandals demonstrate the need for companies to continue to evaluate the effectiveness of their reporting and investigations channels, especially in the aftermath of an investigation
- Multinational organisations must be able to evaluate and understand how cultural drivers shape attitudes toward compliance across global locations

Referenced in this article

- Avianca Holdings bribery scandal
- Airbus bribery scandal
- Operation Car Wash (Petrobras)
- US Department of Justice Criminal Division

Introduction

As anyone who has led a company through an investigation can attest, conducting a thorough investigation can be expensive, time-consuming and difficult while maintaining normal business operations. In the worst cases, investigations can be devastating to a company's reputation and long-term financial viability. No matter the scale of an investigation, companies are often left wondering why misconduct occurred and how it could be prevented in the future. When companies handle remediation appropriately, not all that comes out of an investigation has to be negative. We have seen many instances where companies successfully leverage the 'lessons learned' from the investigation and reinforce the importance of building a sustainable culture of ethics and compliance during the remediation process, resulting in a stronger and more resilient organisation.

The Department of Justice (DOJ) has also placed increased emphasis and weight on effective remediation and noted it as a key hallmark of a best-in-class compliance programme.[1] Therefore, moving forward requires organisations to think strategically and demonstrate thoughtfulness, patience and persistence in properly closing out the investigation and developing clear, pragmatic remediation plans for addressing the factors that allowed the misconduct to occur. Following an investigation, it is important to ensure ongoing review and enhancement of internal controls, especially those that related to the historical conduct in question. Forward-thinking companies can also use the investigation as an opportunity to assess broader areas of compliance that impact the organisation by demonstrating a compliance-minded tone at the top and in the middle, and a robust risk assessment process to owners and shareholders.

In this chapter, we describe factors that companies should consider as an investigation draws to a close and practical suggestions for designing effective remediation plans and a strong control environment. We suggest best practices for companies to ensure they are well-positioned to detect and investigate future fraudulent or non-compliant behaviour. We also highlight how companies need to consider the unique challenges the covid-19 pandemic presents, as challenging market conditions and disruptions to the business environment necessitate a nuanced approach to strengthening a company's compliance environment.

The processes and best practices we describe are applicable to companies located anywhere who are looking to move forward following a myriad of situations, from employee theft, money laundering and fraud allegations to environmental, regulatory or improper accounting concerns. For the purposes of this chapter, we provide examples and cultural considerations specific to companies based or operating in the Americas and have chosen to highlight examples primarily focused on bribery and corruption given the current relevance of these issues. Headline-worthy scandals in countries within South America and Latin America continue to sweep newspapers, including Avianca Holdings who announced in late 2019 that it was investigating potential

1 'Evaluation of Corporate Compliance Programs', pg. 26. US Department of Justice Criminal Division. Updated June 2020.

anti-bribery violations by its employees who provided free airfare and upgrades to public officials.[2] In addition to Avianca's internal investigations, Airbus' recent bribery and corruption settlement spawned a raid of Avianca's offices by Colombian authorities, as information surfaced that Airbus intended to use an intermediary to bribe an Avianca executive in order to facilitate the sale of an Airbus aircraft.[3] Such misconduct demonstrates the need for companies to continue to evaluate whether their compliance programmes are designed to effectively prevent, detect and deter fraudulent behaviour, especially in the aftermath of an investigation.

Closing an investigation

We have too often seen companies rush to move on from an investigation without taking steps to properly close out the investigation. When closing an investigation, it is important that pertinent information be identified, captured and communicated in a form and time frame that enables employees to carry out their responsibilities to establish, enhance and monitor controls and rebuild a more efficient, effective and compliance-minded organisation.

Regulatory compliance considerations

Companies should consult counsel and carefully evaluate and delineate applicable regulatory requirements. Companies are often subject to multiple jurisdictions and regulations and this process can be challenging. For example, jurisdictions and regulatory bodies have varied and nuanced requirements related to self-disclosure of identified misconduct and sometimes self-disclosing to one regulator necessitates further disclosure to additional regulators. While a full analysis of the requirements would necessitate discussion beyond the scope of this chapter, we raise this as an example of a regulatory requirement companies should consider as the investigation progresses.

Disciplinary actions

Enforcing disciplinary actions is an important consideration when concluding an investigation. DOJ guidance indicates that disciplinary actions should be 'commensurate with the violations' and that 'swift consequences' should follow instances of unethical conduct.[4] Additionally, disciplinary actions should be applied consistently across global locations and in accordance with applicable regulations. A standardised approach illustrates to employees that the company takes misconduct seriously and also is relevant to preventing a liability that could result from discriminatory applications of penalties. It further serves as a positive reinforcement to the company's tone at the top, when the policy is applied evenly and fairly regardless of the person's position within the organisation. Additionally, given the myriad of changes in the way business

2 'Latin American Airline Group Notifies U.S. Authorities of Foreign Bribery Investigation', *The Wall Street Journal* (https://www.wsj.com/articles/latin-american-airline-group-notifies-u-s-authorities-of-foreign-bribery-investigation-11565900543?mod=article_inline).

3 'Airline Group's Offices Raided by Colombian Prosecutors', *The Wall Street Journal* (https://www.wsj.com/articles/airline-groups-offices-raided-by-colombian-prosecutors-11581720710).

4 'Evaluation of Corporate Compliance Programs', pg. 13. US Department of Justice Criminal Division. Updated June 2020.

is conducted during the covid-19 pandemic, companies should evaluate if the outcome of an investigation requires additional compliance communication to all employees reiterating the culture of compliance, a concept that may not be top of mind when employees are working remotely with limited to no interaction with managers and executive leadership.

Investigation reporting

Documenting the outcome of an investigation, including the nature and type of report, can present its own complications and challenges. Many factors, such as regulatory or other disclosure obligations, the involvement of multiple regulators, pending or anticipated litigation, potential investigation outcomes, whistleblower involvement, privilege concerns and budgets, will impact the decision on the type of and level of detail in any type of investigation report that is ultimately prepared.

A formal written report has many advantages, such as providing the company a platform for controlling the narrative and documenting the investigation in a manner that satisfies regulators and provides evidence the company took the issue seriously, performed steps to thoroughly investigate allegations and documented remediation. However, it is imperative that counsel is consulted before any report is prepared. In the current enforcement environment, any formal report should be prepared with the assumption that it could end up in the hands of prosecutors and regulators, who may not view the steps taken and results in the same light as the companies. Additionally, disclosure of a written report might lead to adverse consequences such as waiver of the attorney–client privilege and disclosure of information detailing a 'road map' to adversaries in follow-on litigation. It is important to understand the type of reports the investigators intend to issue and whether the report will be available publicly.

The internal or external investigators involved in the investigation have a front-line view of the process failures, misconduct and compliance weaknesses that allowed the alleged misconduct to occur. We strongly encourage companies to ensure that the investigators provide a debrief during the reporting phase – whether through a formal written investigation report, a separate standalone deliverable or an oral readout – that includes the investigators' assessment of any control deficiencies, gaps in the control environment and opportunities to improve processes in line with best practices that came to light during the course of the investigation. This feedback will be essential in developing a remediation plan to help the company ensure a robust control environment moving forward.

Developing and executing a remediation plan

During and following an investigation, companies should develop a remediation plan that seeks to address the conditions that allowed the misconduct to occur. The remediation plan should, at a minimum, incorporate the investigator's observations and suggested recommendations regarding specific control deficiencies. It should also take into consideration the potential impact of covid-19 on the organisations' ability to develop and execute an effective remediation plan (eg, impact of a work from home environment and need for interim remedial procedures due to limitations imposed by covid-19). Given the opportunities that have been created during the pandemic, we strongly encourage companies to take remediation a step further and

use it as a chance to refresh or conduct an assessment of the broader control and compliance environment to illuminate other aspects of the corporate compliance programme that may not be effectively preventing, detecting and deterring misconduct.

Creating an effective remediation plan

Many companies struggle with remediating deficient controls due to issues with the remediation plan itself. A well-designed remediation plan should clearly articulate specific actions the company needs to take to address the identified issues. The plan should be pragmatic and risk-based, anticipating the cost of the control and potential resourcing constraints. Remediation plans should identify milestones with due dates and responsible owners for each action item wherever possible to encourage accountability. The plan should consider 'check in' points when the process owners and operators can discuss with the compliance function best practices, controls that are working and areas that need adjustment. Controls that are too complicated, or that fail to factor the significant changes within the business landscape, are often circumvented or ignored.

Companies should also ensure that the steps in a remediation plan actually mitigate the control deficiency. Companies far too often create 'band-aid' solutions when developing remediation plans due to a lack of understanding of the root cause of an issue or in an effort to demonstrate that a control has been implemented to address the deficiency. The DOJ describes the ability 'to conduct a thoughtful root cause analysis of misconduct and timely and appropriately remediate to address the root causes' as a 'hallmark of a compliance programme that is working effectively in practice'.[5] Far too often, we have seen companies rush to implement a quick fix for an obvious, or superficial, issue rather than taking the time to consider whether there were deeper control failures across a broader range of processes and locations that also require remediation. In recent months, due to covid-19, companies have had to transform how they conduct their day-to-day operations and we have seen that many companies have not had the opportunity to, or have not prioritised, conducting effective root cause analysis or risk assessments to identify the vulnerabilities that may have led to the investigation or may lead to future investigations. Defining effective remediation steps requires thorough analyses of and reflection on the root cause of an issue and consideration of whether control gaps are pervasive across multiple processes or business units.

We will use a brief case study to illustrate how a fictitious company, ZYX Inc (ZYX), should approach remediation following an investigation into the bribery of customs officials through third-party intermediaries (TPIs). Employees of ZYX utilised a recently on-boarded TPI that made improper payments to customs officials in order to facilitate the shipment of ZYX's personal protection equipment (PPE) products. Due to covid-19 related delays and urgency of receiving the PPE shipment, the company performed expedited due diligence for this TPI since they were able to illustrate a recent track record of processing global shipments. ZYX did not have a formal expedited due diligence process in place, and therefore expediting due diligence

5 'Evaluation of Corporate Compliance Programs', pg. 17. U.S. Department of Justice Criminal Division. Updated June 2020.

equated to bypassing established procedures and controls. Additionally, ZYX's due diligence procedure gave the procurement team sole responsibility for performing due diligence, and the compliance and legal teams were never consulted regarding the risks associated with utilising TPIs. Lastly, ZYX did not have a formal process in place to perform ongoing review or monitoring on its TPIs after the initial on-boarding process. Given these significant weaknesses in the due diligence process, a thorough assessment of the TPI involved in the bribery scheme was never performed.

Though certainly not an exhaustive list, the following remediation steps are intended to provide examples of actions the company could take to ensure proper due diligence and ongoing monitoring of third-party intermediaries. These steps take into account the DOJ's recent update in which they specified that prosecutors should assess the company's risk management practices regarding third parties, including whether the company evaluates third-party risk throughout the entirety of the business relationship or solely during the on-boarding process.[6]

- Review the procedural documentation and controls regarding the new vendor on-boarding process to ensure that thorough vendor due diligence is performed on all vendors who may interact with government officials. Additionally, implement a process of compliance and legal review and approve all vendors with exposure to government officials or politically exposed personnel.
- Consider establishing and formalising an expedited due diligence process that allows the organisation to swiftly on-board new vendors under specified circumstances. This should include guidelines around the minimum level of due diligence required at the time of on-boarding, a timeline for when a thorough due diligence should be completed and incorporate approvals from compliance, legal and executive leadership.
- Inventory and risk rank all the vendors who may interact with the government, so transactions with those entities can be subject to additional review or scrutiny. This should be performed not only in response to the investigation, but on a periodic basis.
- Utilising a risk-based approach, perform ongoing anti-bribery and corruption reviews on TPIs with whom the company will continue business relationships. The due diligence should, at minimum, include the following elements:
  - cross referencing against list of entities subject to international economic sanctions or other available lists of high risk entities;
  - understanding ownership structure;
  - identifying government affiliation through ownership or politically exposed personnel; and
  - reviewing litigation profile and adverse media.
- Define events that would trigger a vendor review. These events could include changes in ownership, contract renewal, changes in contracted scope or new information that may change the anti-bribery and corruption risk profile. Compliance and legal leadership should review the due diligence performed and provide final approval.

6 'Evaluation of Corporate Compliance Programs', pg. 8. U.S. Department of Justice Criminal Division. Updated June 2020.

- Formalise the record retention process for the due diligence performed on all vendors and develop systematic tracking to appropriately identify vendors that would be up for review.
- Review anti-corruption compliance policies and procedures and update them as appropriate to ensure clear and consistent messaging.
- Provide anti-bribery and corruption training that includes a robust description of the risks related to TPIs, state-owned entities and a more comprehensive definition of government officials.
- Conduct communications and certifications with vendors, especially TPIs, reinforcing the importance of compliant behaviour, informing them of new and potential requirements, highlighting certain risks and deterring misconduct.

Testing the newly-implemented controls

All internal control systems require monitoring and it is especially important to plan for testing and monitoring newly-implemented or enhanced controls. The monitoring specifications should provide a clear plan to test control, including the frequency of the testing and identifying the person that is responsible for performing the review. Relying on internal audit to perform testing at a later time during a normal course audit is simply not enough, especially for a control that already failed to adequately prevent misconduct. The testing should be performed by a party independent from the control owner and should allow for assessment of 'normal course' behaviour wherever possible.

Continuing with the ZYX Inc case study above, examples of remediation steps ZYX could perform to confirm effectiveness of controls include:

- reviewing the vendor due diligence documentation for vendors on-boarded since the start of the covid-19 pandemic and after the implementation of enhanced policies and procedures to ensure compliance and effective implementation of controls;
- analysing the vendor master file to ensure appropriate risk classifications and that any changes in risk classification appear reasonable, with approval documented; and
- selecting a targeted sample of higher risk vendors to ensure ongoing review and monitoring (eg, vendors involved in the logistics and customs clearance process, especially if more PPE shipments are expected).

Tracking remediation plans through resolution

Companies often fail to follow remediation actions through to closure, especially in the current environment when companies are constantly reinventing and transforming the way they conduct business due to the global restrictions in place to prevent the spread of covid-19. Since the start of the pandemic, we have seen a trend of companies deprioritising or delaying the remediation of identified control gaps to focus on business continuity. While focusing on business continuity is critical, companies should not take the approach that the current business environment is only 'temporary' and should ensure effective remediation of all identified vulnerabilities in a timely manner. If companies fail to conduct effective remediation of identified gaps, they significantly increase their risk of future investigations.

It is essential that companies ensure a strong protocol is in place to follow through on the implementation and track monitoring of recommended remedial measures (including those resulting from the investigation, internal audit and compliance reviews). Remedial measures, the status of their implementation and the process to test the effectiveness of implementation should be memorialised and tracked in a central repository, identifying a responsible party to track the status and having a process in place to test the effectiveness of implementations before considering a remediation 'complete'.

There must also be consequences for a responsible party that fails to meet an assigned due date without a reasonable and plausible explanation. Management should be notified immediately if remedial measures have not been implemented within agreed upon time frames. It may also be necessary to notify the company's compliance officer, the audit committee of the board of directors and the regulators if remedial measures have not been implemented in a timely manner.

Strengthening the organisation and moving forward

A full review of a company's compliance programme includes:

- an assessment of tone at the top;
- performing a gap analysis of the policies and procedures in place;
- performing a refresh of the global risk assessment;
- implementing controls to reduce residual risk; and
- understanding how the company educates employees of key risks and expected behaviour through planned trainings and communications.

Organisations need to ensure that all areas of compliance operate in a holistic, integrated manner in order for a compliance programme to be truly effective. Three areas of a compliance programme that are important to assess following an investigation include assessing the internal audit function, monitoring controls and complaint reporting, and investigation channels. These areas are important because detecting control weaknesses, identifying potential misconduct at the earliest instance and effectively investigating issues that may arise in the future are critical to maintaining adequate controls and an effective compliance programme. This point is further emphasised in the current economic environment in which we are seeing organisations implement cost-saving measures resulting in budget and headcount reductions within their primary lines of defence, including compliance and internal audit. Based on our experience, economic downturns typically increase an organisation's exposure to fraud and misconduct and short-term cost savings eventually create gaps within the overall compliance programme that can result in costly and time consuming investigations down the road. This trend of reducing budget and headcount is also contrary to the DOJ's recent guidance, which emphasises adequate staffing, with resources equipped with appropriate skill sets, to ensure an effective compliance programme.[7]

7 'Evaluation of Corporate Compliance Programs', pg. 11-12. U.S. Department of Justice Criminal Division. Updated June 2020.

Assessing the internal audit function

Internal audit's mandate is not necessarily to detect all instances of fraud – intentional subversion of controls can be very difficult, if not impossible, to detect – but following an investigation, it is important to consider whether internal audit should have identified the misconduct. This assessment is especially critical if the misconduct was pervasive throughout the organisation, occurred over a long period of time or the fraudulent behaviour exhibited a number of 'red flags' that followed predictable fraud patterns (eg, large round dollar payments with vague descriptions to new vendors).

A well-designed, robust risk assessment should feed into audit planning by highlighting key risk areas (eg, related to geographic area, business unit, industry-specific risks). Internal audit should consider these risks when building the annual audit plan for the company. Internal audit teams often build audit procedures that focus on assessing controls (as expected), but miss the mark in designing procedures to pick up specific risks (eg, related to bribery and corruption). Additionally, since audit plans are typically finalised during the start of a fiscal year, they are likely to miss the mark on the new risks and potential control gaps created by the rapidly changing business landscape since the start of the covid-19 pandemic. As a best practice we have seen companies re-evaluate their audit plan and design specific audits to cover controls that may be affected by work from home arrangements. Companies should also ensure that internal audit are adequately staffed with team members possessing the requisite experience and skill set to perform assessments related to specific risks and that all team members receive continued training. Internal audit also needs to have visible support from the highest levels of leadership to be effective. Limited access to key employees, data and documentation severely restricts internal audit's ability to conduct meaningful and thorough assessments. Internal audit should have access to all of the information they require to assess control adequacy and remediation efforts, and business units should respond swiftly to requests and directives. When business leaders are dismissive towards internal audit, business units can feel empowered to ignore audit findings and suggested remediation recommendations.

In the ZYX Inc example, the company should consider whether internal audit identified any related issues previously (eg, insufficient vendor due diligence, lack of ongoing vendor monitoring) and recommended remedial measures similar to those we outlined above. If so, then ZYX Inc's leadership may have a problematic attitude toward internal audit or the organisation may be deficient in following through with remediating audit findings. If internal audit had not, however, identified similar issues, ZYX Inc should assess whether the annual audit programme provides adequate geographic, business unit, product and key risk coverage, whether the auditors are adequately skilled and trained to assess risks and whether audit procedures are adequately designed to detect the type of control weaknesses identified.

Data analytics for ongoing monitoring

According to the DOJ, organisations need to 'ensure that the organisation's compliance and ethics programme is followed, including monitoring and auditing to detect criminal conduct', and 'evaluate periodically the effectiveness of the organisation's' programme.[8] Monitoring entails testing the effectiveness of key controls, including assessing whether the controls are functioning as intended and employees are adhering to procedural requirements. The ongoing nature of monitoring allows for earlier detection of misconduct (rather than waiting for internal or external auditors to perform testing on a prescribed time frame). In line with the guidelines presented above, organisations should have clear mechanisms in place to ensure identified deficiencies are adequately and promptly remediated. The risk assessment process should focus the compliance department toward the most critical areas to prioritise for monitoring. Monitoring procedures are often identical to common audit procedures and may entail reviewing transaction details and related documentation for discrepancies, duplication, errors, policy violations, missing approvals, incomplete data, dollar or volume limit errors, or other potential internal control failures.

The best continuous monitoring programmes leverage data analytics and allow the monitoring team to quickly and consistently focus on the highest areas of risk, reducing the noise of volumes of data. Data analytics facilitates the review of broad data sets that may not be feasible through manual review. Metrics stemming from data analytics can flag key risk areas such as high risk payments, fluctuations in payments, suspicious large round dollar payment amounts or payments to unusual accounts. Data analytics facilitate comparative analysis, simple visualisation of key data and can be used to inform risk-based sample selection for transaction-based testing by highlighting transactions that follow certain patterns (eg, high, rounded dollar payment recorded for a new vendor in the general ledger account). Companies can also develop ways to visualise data through dashboards and sophisticated visualisation tools that will allow the companies' management to quickly delve into large volumes of data to explore trends more deeply (eg, spikes of activity in a specific region).

Companies can leverage data analytics to monitor transactions real time and identify transactions with similar fact patterns. Monitoring procedures can include developing advanced queries to generate lists of data (payment activity, list of vendors, among others). These lists can be used to select high-risk accounts for testing, payments to entities with similar names and vendor risk ratings. ZYX Inc could leverage bespoke data analytics to identify transactions following a similar pattern that exhibit the following attributes:

- transactions recorded to accounts or vendors with typically low volume of monthly activity;
- transactions recorded to selected 'high-risk' accounts that display certain characteristics, such as round dollar amounts, being above a certain threshold, missing an invoice number and potentially duplicative; and
- changes in risk rating of vendors in the master vendor file from prior months.

8 'Evaluation of Corporate Compliance Programs', pg. 25. US Department of Justice Criminal Division. Updated June 2020.

Complaint reporting and investigation channels

While organisations would, of course, prefer to not have misconduct, it is inevitable that in a large, global organisation an allegation requiring further investigation will arise. What is worse than an investigation initiated by an ethics hotline complaint? An investigation initiated by the government based on whistleblower complaints, because the company did not take a complaint seriously or failed to conduct an effective investigation of an allegation. Recent international public scandals demonstrate the need for companies to continue to evaluate the effectiveness of their reporting and investigations channels, especially in the aftermath of an investigation. Petrobras, the company at the centre of Operation Car Wash, was reportedly revisiting its treatment of whistleblower complaints.[9] It has been reported that Petrobras had received a whistleblower complaint regarding potential corruption in its oil trading business in 2012, but failed to stop the improper activity.[10]

Companies should have an ethics hotline in place that allows any employee, vendor or other external party to make an anonymous complaint. The hotline should be available 24/7, reachable by multiple channels that include a local telephone number, online portal and email address, and must allow tipsters to submit a complaint in the local language. In the current environment, companies should ensure their hotlines are operating effectively and there are protocols and redundancies in place to ensure there is not a lapse in coverage. However, simply setting up the hotline is not enough, companies must take appropriate steps to advertise the hotline and ensure that all relevant parties understand how to submit a complaint and feel comfortable submitting a complaint without fear of retaliation. Organisations must also reflect on the impact that culture has on an individuals' willingness to use the hotline. The level and type of messaging a company creates to advertise the hotline may need to be different to educate employees who may have preconceived notions or cultural expectations about whether it is appropriate to raise an allegation against one's supervisor, or trusting whether the allegation, if raised, will actually be acted upon without retaliation. Given the recent emphasis on corruption in Brazil and prevalence of ongoing investigations, we have used Brazil as an example on cultural considerations. It is well-recognised that the Brazilian culture 'by and large, is not favourable to whistleblowing behaviour'.[11] Lack of whistleblower protections as well as a hierarchical society where the distribution of power is imbalanced contribute to a general fear of retaliation.

Additionally, organisations need to ensure that processes are in place to effectively, thoroughly and promptly investigate any allegations submitted to the hotline. We have seen that the lack of a strong investigations process can undermine a company's efforts to implement

9 'Brazil's Petrobras revisits whistleblowers in wake of trading scandal', (https://www.reuters.com/article/us-petrobras-corruption/brazils-petrobras-revisits-whistleblowers-in-wake-of-trading-scandal-idUSKCN1RY1DN).

10 'Exclusive: Petrobras ignored warnings about fuel broker implicated in graft probe', https://www.reuters.com/article/us-petrobras-corruption-exclusive/exclusive-petrobras-ignored-warnings-about-fuel-broker-implicated-in-graft-probe-idUSKCN1TE1B4.

11 Sampaio, Diego BD, 'Speak Now or Forever Hold Your Peace: An Empirical Investigation of Whistleblowing in Brazilian Organizations' (https://pdfs.semanticscholar.org/492a/47ac593f21b7b20bc1861b50390186bcc8f8.pdf).

and advertise a hotline, as employees can adopt a 'why bother' attitude if they feel allegations raised will not be taken seriously, investigated on a timely basis or that the company would not take appropriate disciplinary action when warranted. Investigators should also possess the requisite skill sets to investigate the allegation at hand (eg, forensic accounting skills are ideal for investigations into improper payments, while an allegation regarding sexual harassment will necessitate a human resources-oriented investigator).

A well-designed investigations process should complement other key compliance processes, including, for example, steps to ensure that any remedial actions required as a result of an investigation are carried through to completion and appropriate disciplinary measures result from the investigation when warranted. Companies should also consider the nature, frequency and outcomes of their own investigations, as well as those of their peers, when evaluating the company's tone at the top, performing risk assessments and preparing annual audit plans.

Conclusion

We recognise that establishing, maintaining or changing an overall culture of compliance requires a sustained effort. In recent months we have seen covid-19 bring about inconceivable changes to the business landscape, further reiterating that a one-time focus on the ethics and values will not be enough to achieve a corporate culture that truly embraces ethical behaviour. Organisations failing to align business strategies and operating decisions, including personnel decisions, to desired ethics and values are at potential risk of extraordinary financial and reputational costs. As such, the compliance function must have the stature and authority, support of senior leadership and necessary funding to successfully establish, implement and monitor an effective compliance programme. In conclusion, it is apparent there are several courses of action, factors, nuances and underlying currents that need to be navigated post any investigation. The recommendations in this chapter are offered as a compass on that journey. It is best to charter one's course carefully to truly strengthen the organisation and allow it to surge ahead, especially during these uncertain times.

The authors would like to acknowledge Aeriel Davis (senior associate) and Jaime Jerez (senior associate) for their contributions to this chapter.

Frances McLeod
Forensic Risk Alliance

Frances McLeod is a founding partner of Forensic Risk Alliance (FRA) and head of its US offices. She is a former investment banker and has over 25 years of experience advising diverse clients on sanctions, anti-corruption, fraud, internal controls, asset tracing and money laundering issues.

Frances has been deeply involved in all of FRA's compliance monitorship work, to include US Department of Justice and Securities and Exchange Commission FCPA monitorships, a New York Department of Financial Services bank monitorship, the Ferguson City monitorship, a Public Company Accounting Oversight Board monitorship and a Department of Justice fraud-related monitorship.

Frances has extensive experience in addressing complex international data-transfer issues whether in regulatory investigations or cross-border litigation. She led the FRA team responding to anti-corruption investigation data requests in all jurisdictions for Alstom in the United States, United Kingdom, Brazil, Indonesia, Poland, Sweden, among others, which included addressing French data privacy and blocking statute issues. She is leading FRA's General Data Protection Regulation compliance initiative, leveraging FRA's decades of experience in addressing data protection issues in cross-border litigation and investigation.

Jenna Voss
Forensic Risk Alliance

Jenna Voss is a partner at Forensic Risk Alliance with extensive experience providing guidance to clients in sensitive cross-border matters across multiple industries. She leads teams in performing anti-bribery and corruption compliance reviews and investigations, conducting white-collar investigations and providing accounting expertise on litigation matters. She has led teams globally and has significant experience in the Americas, including in the United States, Mexico, Brazil and Canada.

Jenna recently led a global team in performing a multi-year forensic assessment at the direction of the monitor of a Brazilian-based company that engaged in misconduct related to bribery and corruption. Previously, Jenna supported the Mexico operations of a biomedical devices client in enhancing its anti-corruption compliance programme while under a multi-year monitorship. Jenna also has experience conducting whistleblower investigations, leading anti-money laundering assessments, performing accounting and anti-corruption due diligence, building complex financial models and advising financially troubled companies in bankruptcy and restructuring situations.

She is a certified public accountant, certified fraud examiner, certified anti-money laundering specialist and certified in financial forensics and holds master's degrees in business administration and accounting.

Umair Nadeem
Forensic Risk Alliance

Umair Nadeem is a director at Forensic Risk Alliance with extensive cross-industry experience in providing consulting and investigative services regarding issues of fraud and misconduct including: financial statement fraud, bribery and corruption, asset misappropriation, regulatory enforcement actions and the assessment of financial and legal risks relative to fraud and poor internal controls. Umair has a proven track record of leading large scale investigations, corporate monitorships and providing accounting expertise on litigation matters across the Americas, Europe, Middle East and Africa.

Umair most recently concluded an in-country investigation in the Middle East to resolve allegations of bribery and corruption through third-party intermediaries, and is currently leading a cross-border team providing forensic accounting support to the DOJ appointed Monitor of a global financial institution.

Umair has a degree in business administration in finance from the University of Texas. He is a certified fraud examiner and a board member of the Houston chapter of the Texas General Counsel Forum. He is also an active member of the Association of Certified Fraud Examiners and the Society of Corporate Compliance and Ethics.

Forensic Risk Alliance is a global market leader working with clients to identify, analyse and mitigate the risks associated with international regulatory compliance obligations, litigation, internal and external multi-jurisdictional investigations. Unlike traditional accounting firms, we operate purely in the forensic space and generally have no conflicts. Our highly skilled and sophisticated team comprises forensic accountants, former investment bankers, financial and data analysts, legal and litigation support professionals, database architects, electronic discovery and collection experts, software engineers and certified computer examiners. This includes individuals who have worked for the UK Serious Fraud Office, US Securities and Exchanges Commission and US Federal Bureau of Investigation.

As internationally recognised specialists in multi-jurisdictional investigations, we bring a high level of confidence to clients by providing clear, robust and candid advice that is trusted by clients, regulators, courts and enforcement agencies.

We have extensive cross-sector and cross-border experience and scalability anywhere in the world. Our globally integrated teams have worked in more than 75 countries – both developed economies and emerging markets.

We offer extensive data privacy and protection and jurisdiction-specific experience (eg, blocking statutes, banking and state secrecy laws, commercial secrecy, global privacy legislation and security risks, state sponsored and other hacking, leaks, data loss, and excessive data retention).

Complex data analytics, information technology and data management are at the core of our foundation. Our data analytics team seamlessly integrates with our forensic accounting, digital forensics and eDiscovery teams to offer creative analytical and visualisation solutions tailored to client needs.

Audrey House
16-20 Ely Place
London EC1N 6SN
United Kingdom
Tel: +44 20 7831 9110
www.forensicrisk.com

Frances McLeod
fmcleod@forensicrisk.com

Jenna Voss
jvoss@forensicrisk.com

Umair Nadeem
unadeem@forensicrisk.com

The *Americas Investigations Review 2021* contains insight and thought leadership from 28 pre-eminent practitioners from the region. Across 11 chapters, spanning around 160 pages, they provide an invaluable retrospective and primer.

Together, these writers capture and interpret the most substantial recent international investigations developments of the past year, with footnotes and relevant statistics. Other articles provide valuable background so that you can get up to speed quickly on the essentials of a particular topic.

This edition covers Brazil, Mexico and the United States – each from multiple perspectives, and has overviews on the Department of Justice's use of tools that are not the Foreign Corrupt Practices Act; on evidence gathering; and on how to ensure that history does not repeat – the art of learning the right lessons as an investigation winds down.

Visit globalinvestigationsreview.com
Follow @GIRAlerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-267-1