

The DOJ, the FCPA, and the Impact of the Yates Memo: What It All Means, and How to Avoid Violations Using Data Analytics

A WHITE PAPER FROM OVERSIGHT

The Mission Statement of the DOJ: To enforce the law and defend the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans¹

Fighting corporate fraud and misconduct has always been a top priority for the Department of Justice (DOJ). In 1977, Congress passed the Foreign Corrupt Practices Act (FCPA) to punish bribery intended to influence the decisions of foreign officials. Any violation is punishable by criminal and civil penalties that can be applied against both companies and individuals.

The FCPA makes it a crime to: 1) make a payment of, offer or promise to pay, or authorize a payment of money or anything of value, directly or indirectly; 2) to any foreign official, politician,

party official, candidate for office; 3) with a corrupt intent; 4) for the purpose of influencing one of these person's official acts or decisions in violation of his or her lawful duty; 5) in order to assist in obtaining or retaining business.²

Examples of FCPA accounting violations include failing to implement internal controls, to keep accurate books and records, to conduct appropriate audits of payments, and to implement sufficient anti-bribery compliance policies.³

The repercussions resulting from a confirmed FCPA violation



can be substantial. Since the law was passed, billions of dollars in financial penalties have been paid to resolve FCPA violations. In 2021 alone, the DOJ and Securities and Exchange Commission (SEC) brought actions against four companies and imposed financial penalties totaling \$282 million. The year before, 12 companies paid a record \$6.4 billion to resolve FCPA cases.⁴

Penalties can be avoided with the proper controls in place. In fact, if a company conducts any business overseas, they should have a checklist for testing their FCPA controls similar to the following:⁵

- Identify the nature of your business and all sectors in which you operate.
- Identify all nations in which you operate and/or engage in commerce.
- Research the Corruptions Perception Index published by Transparency International — a global coalition with a mission to stop corruption and promote transparency — for each nation in which you operate and/or engage in commerce (www.transparency.org).
- Identify all public/governmental agencies to which you market and/or sell products and services.
- Inventory the strengths and weaknesses of your corporate internal controls.
- Identify all executives and employees responsible for compliance with federal statutes and regulations.
- Revisit record keeping and accounting procedures for all international transactions to ensure accurate characterization of all expenditures.
- Implement an anonymous hotline for employee concerns with measurable follow-up and accountability for addressing each call in a timely manner.
- Revisit the content of employee compliance training on an annual basis.
- Develop an ongoing relationship and exchange of information with knowledgeable external legal counsel.

A thorough review of the current compliance program is another way to mitigate the risk of an FCPA violation.

“HALLMARKS OF EFFECTIVE COMPLIANCE PROGRAMS.”

1. Commitment from Senior Management and a Clearly Articulated Policy Against Corruption
2. Code of Conduct and Compliance Policies and Procedures
3. Oversight, Autonomy, and Resources
4. Risk Assessment
5. Training and Continuing Advice
6. Incentives and Disciplinary Measures
7. Third-Party Due Diligence and Payments
8. Confidential Reporting and Internal Investigation
9. Continuous Improvement: Periodic Testing and Review
10. Mergers and Acquisitions: Pre-Acquisition Due Diligence and Post-Acquisition Integration
11. Investigation, Analysis, and Remediation of Misconduct⁶

THE YATES MEMO

“One of the most effective ways to combat corporate misconduct is by seeking accountability from the individuals who perpetrated the wrongdoing,” according to the DOJ.⁷

To address this issue, in September 2015, Deputy Attorney General Sally Q. Yates issued a memorandum entitled, “Individual Accountability for Corporate Wrongdoing,” now commonly known as the Yates Memo.

Organizations governed by the FCPA were immediately impacted when the [Yates Memo](#) was first published. After years of pursuing settlements with corporations over individuals, the DOJ and Securities and Exchange Commission (SEC) shifted their focus to prosecuting individuals over corporations.

The issuance of the Yates Memo was meant to deter future misconduct, ensure the proper parties are held responsible for their actions, and promote the public’s confidence in our justice system. The DOJ made it clear they would no longer offer non-prosecution and delayed-prosecution alternatives unless a corporation self-discloses and agrees to assist in the prosecution of individuals. They also stressed the importance for companies to ensure their FCPA compliance programs were in line with DOJ’s expectations to implement the monitoring of all transactions.

REVISIONS IN GUIDELINES

In the past couple of years, there has been a shift of focus when evaluating corporate compliance programs. The June 2020 revision to the DOJ compliance guidelines requires prosecutors to investigate how a company is tracking the functionality of its operations and compliance efforts. Part of this determination is done by looking at the company’s use of data analytics.

Using data analytics could help continuously monitor and ensure third-party compliance by identifying risks as they emerge. This gives companies more time to evaluate and determine the best course of action to mitigate potential liability.⁸

One critical area organizations struggle with is **monitoring travel and entertainment expenses, reimbursements, and purchases that pose FCPA risk**, simply because of the sheer volume of transactions that occur every day.

COVID 19 IMPACT

The global pandemic created many challenges for businesses all around the world. However, it did not slow down the enforcement actions the government imposed for FCPA violations.

While there were many large settlements during year one of the pandemic, in October 2020, a record-breaking \$3.3 billion settlement with Goldman Sachs clearly demonstrated how a business’s compliance program must evolve amidst external stressors. Charles Cain, chief of the FCPA unit of the SEC, stated, “When compliance is under the most pressure from the organization is when it must work best.”⁹

The overall impact of COVID did not decrease the government’s expectations of compliance. Instead, it reiterated the importance of resourcing, empowering, and preparing an effective compliance department.

Three main concepts for businesses to recognize as their compliance programs evolve and respond to different business environments resulted from the Goldman settlement:

- 1. Compliance cannot be cyclical, seasonal, or “contextual.”** Controls must be tested for effectiveness regardless of economic conditions, and nothing should compromise compliance planning and review.
- 2. Compliance organizations must adapt and continually evaluate sources of risk.** Informal methods may not be effective, so utilizing technology and data to identify potential issues is extremely important.
- 3. Compliance is not effective just because the compliance department detects potential issues.** Even as businesses are cutting back on resources, compliance personnel must be able to investigate and stop questionable business practices in a continuous manner.¹²

A RENEWED COMMITMENT

Fast-forwarding to 2021, six years after the Yates Memo was first published, the DOJ announced that it would be renewing its commitment to combatting white collar crimes. In doing so, they also made it clear that any financial pressures and business disruptions would not be an acceptable excuse for a poorly performing compliance program.

Part of this renewed commitment would require the Department to take a fresh look at the standards and practices of all aspects of corporate enforcement, and to provide additional resources to their prosecutors. This included the formation the Corporate Crime Advisory Group to propose revisions or make recommendations to existing policies and procedures.

The DOJ also indicated that there will be zero tolerance for repeat offenders. Specifically, more emphasis will be placed on all past infractions (criminal, civil and regulatory) when prosecutors are making settlement decisions, even when past discretions are unrelated to current allegations.

Principal Associate Deputy Attorney General (“PADAG”) John Carlin noted in October that there would be a “surge of resources for corporate enforcement.” This surge would facilitate the use of data analytics tools that would be shared among regulatory agencies to identify potential misconduct. Carlin advised how corporations should take advantage of similar tools in their compliance programs.¹⁰

The current key areas of interest for the DOJ are mergers and acquisitions, continuous improvement through data analytics, and third-party monitoring. As they are relying more and more on data analytics for investigation, the Department expects companies follow their lead. This would require sufficient resources to monitor and act upon any issues identified through data analysis.

In October, Deputy Attorney General Lisa Monaco warned that a corporate culture that
“fails to invest in compliance ...leads to bad results.”¹¹

PAST AND CURRENT CASES

Despite the criticism for pursuing settlements with organizations, the costs for FCPA violations prior to the issuance of the Yates Memo were significant, both in terms of dollars and damage to a company’s reputation.

- **Hewlett-Packard Co.:** paid \$108 million in April 2014 to settle charges of bribery activities in Poland, Russia and Mexico.
- **Avon Products:** paid \$135 million to settle charges brought by the DOJ and SEC that arose from a multi-year bribery probe.
- **Goodyear Tire & Rubber Co.:** paid more than \$16 million to settle SEC charges that subsidiaries in Kenya and Angola paid bribes to increase tire sales.
- **FLIR Systems Inc.:** paid \$9.5 million to settle bribery charges involving expensive trips and gifts given to Middle Eastern government officials.

There are other precedents that demonstrate the DOJ’s willingness to only prosecute an individual if it feels the organization provides an acceptable level of cooperation. For example, in June 2015, the DOJ announced publicly that it would not prosecute a company that cooperated in building a case against a former officer. After Joseph Sigelman, PetroTiger’s co-founder and former chief pleaded guilty to one count of conspiracy to violate the FCPA, the DOJ issued a statement that concluded:

“Based on PetroTiger’s voluntary disclosure, cooperation, and remediation, among other factors, the department declined to prosecute PetroTiger.”

LESSONS LEARNED FROM MORGAN STANLEY

The first time the DOJ issued a public declination in an FCPA case was in April 2012. Garth Peterson, Morgan Stanley’s former managing director and real estate chief in China, pleaded guilty to evading the company’s internal controls. The DOJ cited the fact that Morgan

Stanley voluntarily disclosed the matter and cooperated throughout the department’s investigation as the reasons for its decision not to bring any enforcement action against the company.

In fact, the Morgan Stanley case can serve as the model for any organization to follow because it demonstrates the need to implement

and follow best practices such as:

Document everything: Morgan Stanley maintained a system of internal controls meant to ensure accountability for its assets and to prevent employees from offering, promising or paying anything of value to foreign government officials.

Conduct regular program auditing: Reviewing and updating its internal policies enabled Morgan Stanley to ensure all policies and procedures were being followed, eliminating the risk of non-compliance or FCPA risk.

Educate employees: According to court documents, between 2002 and 2008, Morgan Stanley trained various groups of Asia-based personnel on anti-corruption policies more than 50 times. In fact, Peterson received training seven times and was reminded him to comply with the FCPA at least 35 times.

Implement global financial systems controls: Morgan Stanley provided documentation that compliance personnel regularly monitored transactions, randomly audited particular employees, transactions and business units, and tested to identify illicit payments.

In its first FCPA Settlement of 2022, the DOJ has re-emphasized that it will not be backing down on enforcement. Seoul-based KT Corporation (KT Corp.), South Korea's largest telecommunications operator, will pay \$6.3 million to resolve charges that it violated the FCPA by providing improper payments for the benefit of government officials in Korea and Vietnam.

According to the SEC press release, the company "lacked sufficient internal accounting controls over charitable donations, third-party payments, executive bonuses, and gift card purchases." This lack of internal controls led to significant compliance failures and FCPA violations.

The SEC also noted the company "had no relevant anti-corruption policies or procedures with respect to donations, employment candidates, vendors, subcontractors, or third-party agents." KT Corp's misconduct amounted to a violation of the books and records and internal accounting controls provisions of the FCPA. The company's remedial acts and cooperation prevented a more substantial civil penalty.

DATA ANALYTICS AND COMPLIANCE

A major gap for most organizations is an inability to accurately and consistently identify patterns of inappropriate behaviors in travel, entertainment and purchasing that pose FCPA risk. The sheer volume of transactions and the ever-growing stores of information to monitor makes it difficult (if not impossible) to identify patterns of behavior via traditional analytical approaches that can only examine one transaction at a time, cannot identify patterns of behavior, and are only capable of detecting large glaring issues. As a result, bad actors fly under the radar and too often get away with policy violations. After all, it's hard to self-disclose when you don't know what's going on.

Also, consider the fact that transactions are rarely black or white, bad or good. They can often fall into a gray area that includes considerations such as the employee, the attendees, the merchant, transaction type, vendor type, the country where the transaction occurred, the home country of the employee, etc.

Additionally, providing investigators with a "slice in time" sample will no longer cut it. An organization must demonstrate it monitors 100 percent of all transactions and does not just take samples to analyze.

OVERSIGHT'S APPROACH TO MITIGATING FCPA RISK

Oversight for Anti-Bribery & Corruption Monitoring is an automated transaction monitoring solution that addresses three specific areas of best practice:

1. Continuous monitoring of transactions and activities for improper behavior.
2. Performing compliance audits around travel & entertainment (T&E) and payables (AP) transactions.
3. Reinforcing policy compliance.

Oversight provides a centralized transaction monitoring system that automatically identifies risky activities and facilitates efficient resolution of any issues. Our analytics look for behaviors or patterns of FCPA risk across expense reports and card transactions in T&E, or invoices and payments in AP.

Oversight's library of analytics looks across multiple dimensions including employees, attendees, vendors, and countries over an extended time horizon. This can pinpoint employees exhibiting patterns of potentially improper behavior or collusion that are difficult to detect in traditional FCPA monitoring and audit approaches. From this analysis, we present Anti-Bribery & Corruption Monitoring risk in the form of cases/exceptions needing further investigation and resolution.

Oversight enables clients to easily demonstrate to the executive team and board, and to government agencies, if necessary, that they are proactively monitoring their business transactions for Anti-Bribery & Corruption Monitoring risk and acting on the exceptions.

A continuous transaction monitoring solution such as Oversight's is an important part of an effective compliance program addressing the DOJ's guidelines for compliance monitoring, communication with employees, compliance evidence, and audit trails.

Leveraging Transparency International's Corruption Perception Index and the CIA or Dow Jones Politically Exposed Persons databases, Oversight identifies high-risk transactions in T&E based on factors including the employee, the attendees, the merchant, the vendor, and the country where the transaction occurred. Oversight then combs through transactions for FCPA-specific keywords such as ministry, facilitation fee, consulting fee and other suspicious terms. Multiple languages are also included in our keyword analysis.

Within Payables, Oversight evaluates the type of transaction, the vendor, and the country where the transaction occurred using the Corruption Perception Index, PEP lists, and FCPA specific key words. Based on political exposure, Oversight also identifies voucher outliers, unusual vouchers or payments, split invoices, and high-risk vendors.

Oversight automatically prioritizes exceptions, highlighting the highest risk countries, employees, spend categories, merchants, and vendors to streamline the review process. Compliance auditors access these exceptions through a secure web-based portal where they can leverage the built-in case management functionality to communicate, collaborate, and act on the findings.

Oversight maintains a permanent, tamper-proof audit log that automatically documents the steps taken to resolve issues. This ensures you can effectively address anti-bribery and corruption risks.

SUMMARY

- Oversight's library of analytics take a risk-based approach to identify anomalies that may suggest FCPA concerns.
- With Oversight's built-in workflows, any actions taken during the review and resolution of potential violations are recorded automatically. Because these workflows are retained indefinitely, the records provide a defensible audit trail demonstrating to all stakeholders that there is continuous monitoring of all business transactions.
- Oversight can operationalize compliance efforts to monitor your travel, entertainment, and payables at an affordable price point, and a timeframe that is achievable.
- While there is no guarantee that you will be able to prevent bad actors from circumventing controls, with Oversight you can have a best practice approach to identify possible violations in travel, entertainment, and payables.

ABOUT OVERSIGHT

Oversight's AI audit and risk management platform digitally transforms how organizations monitor, analyze and mitigate their enterprise spend risk – across travel & expense, payables, and general ledger entries. Working across these disparate financial data sources, Oversight leverages patented and proven analytical techniques to automatically uncover fraud, misuse, and errors, as well as hidden risks and patterns that would lead to greater financial loss if left undetected. By identifying process breakdowns and making corrections early, Oversight helps create a culture of compliance that reduces out-of-policy spending by 70% while maximizing audit efficiency and eliminating cash leakage..

To request a demo of Oversight, please visit: oversight.com/book-demo

ENDNOTES

1. <https://www.justice.gov/about>
2. https://www.foley.com/en/files/uploads/FCPA_FAQs-English.pdf
3. <https://www.whistleblowers.org/foreign-corrupt-practices-act/>
4. <https://fcpablog.com/2022/01/03/2021-fcpa-enforcement-index/>
5. https://issuu.com/todaysgc/docs/tgc_sum20_issuu/s/10680790
6. <https://www.justice.gov/criminal-fraud/file/1292051/download> (pages 58-68)
7. <https://www.justice.gov/archives/dag/individual-accountability>
8. <https://www.lexology.com/library/detail.aspx?g=b7991e6e-60bc-4d0a-83ef-3b46f8fc39e4>
9. <https://www.troutman.com/insights/avoiding-contextual-compliance-in-the-year-of-covid-and-beyond.html>
10. <https://www.gibsondunn.com/2021-year-end-update-on-corporate-non-prosecution-agreements-and-deferred-prosecution-agreements/><https://www.jdsupra.com/legalnews/doj-reintroduces-corporate-compliance-4809185/>
11. <https://www.jdsupra.com/legalnews/doj-reintroduces-corporate-compliance-4809185/>
12. <https://www.troutman.com/insights/avoiding-contextual-compliance-in-the-year-of-covid-and-beyond.html>