

MAYER • BROWN

STROZ FRIEDBERG

DIGITAL RISK MANAGEMENT & INVESTIGATIONS

# The Growing Importance of Internal Investigations: Effectively Coordinating a Global Enforcement Approach for your Company

William Michael, Jr.  
J. Gregory Deis  
Mayer Brown LLP

Joseph M. Alesia  
Stroz Friedberg LLC

June 27, 2013

Mayer Brown is a global legal services organization comprising legal practices that are separate entities ("Mayer Brown Practices"). The Mayer Brown Practices are: Mayer Brown LLP, a limited liability partnership established in the United States; Mayer Brown International LLP, a limited liability partnership incorporated in England and Wales; Mayer Brown JSM, a Hong Kong partnership, and its associated entities in Asia; and Tauil & ChequerAdvogados, a Brazilian law partnership with which Mayer Brown is associated. "Mayer Brown" and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.

## Overview

- Key Considerations In Conducting an Internal Investigation
- High Risk Areas
- Multinational Investigations
  - Foreign restrictions on transfer and review of certain information
  - Privilege issues
  - Practical concerns/limitations
- Minimizing Risks Associated With Global Enforcement Actions/Investigations

### Key Considerations



- ◆ Internal investigations have become a recognized practice for businesses, which are required, through a myriad of obligations, to respond to allegations of misconduct in an ever-increasingly complex legal environment.
- ◆ With increased coordination in global enforcement actions by regulators and law enforcement officials, the complexities associated with global investigations have increased exponentially.

## Key Considerations



- ◆ Properly performed internal investigations assist in:
  - determining whether the allegations have substance;
  - who may have been involved and what level of involvement they had;
  - what the proper responses should be and the legal risks associated with failing to respond;
  - how to minimize the regulatory, civil and criminal exposure of the corporation and its senior management; and
  - what, if any, preventive measures are appropriate to prevent repetition of the events in question.

## Key Considerations



### ◆ Duties of Care, Obedience and Loyalty

- Directors and officers owe fiduciary duties to the corporation, including the duties of care, obedience and loyalty.
- The duty of care requires a director to act in good faith and in a manner the director reasonably believes to be in the best interests of the corporation.
- The duty of obedience requires a director to act within the corporation's scope of powers, as set forth by its charter or by the laws of the state of incorporation, and mandates that directors not exceed those powers.
- The duty of loyalty requires that a director act in good faith and that the director not allow personal interests to prevail over the interests of the corporation.

## Key Considerations



- ◆ **Timing of the Investigation**
- ◆ **Scope of the Investigation**
- ◆ **Determining the Investigative Team Members**
  - *Attorneys*
  - *Experienced Investigators*
  - *Industry Specific Experts*
- ◆ **Investigative Methods**
  - *Documents*
  - *Electronic Evidence*
  - *Personal Interviews*

## Key Considerations



- ◆ **Who is the Client?**
- ◆ **Multiple Representations/Common Interest Agreements?**
- ◆ **Who is Provided Details of the Investigation?**
- ◆ **How to Preserve Privilege?**
- ◆ **Written or Oral Report?**
- ◆ **Self-Reporting to Government?**
- ◆ **Collateral Consequences?**

## Corporate Investigation Protocol

- ◆ While two investigations are rarely identical, investigators should tailor and apply certain practices as appropriate, using their best judgment in each situation, to ensure that the goals of every investigation are attained in the most fair, effective and efficient manner possible.
- ◆ An Investigations Protocol fulfills two important purposes.
  - Companies must maintain a process to investigate and remediate allegations of wrongdoing under the federal Sentencing Guidelines and other applicable laws.
  - Demonstrates a commitment to compliance with legal and regulatory requirements.



## Corporate Investigation Protocol

- ◆ Areas a protocol should address
  - Stated purpose
  - Investigative goals
  - Dealing with reports of misconduct
  - Investigative triage
  - Maintaining attorney-client privilege
  - Forming the investigative team
  - Documenting an investigation
  - The investigative plan

## High Risk Areas

- **FCPA**
- **Antitrust/Competition**
- **Money Laundering**
- **False Claims Act**
- **Data Breach**
- **C-Suite Misconduct**

# FCPA



# FCPA



## Overview of FCPA Provisions

- The FCPA prohibits bribery of foreign public officials and requires issuers to maintain accurate books and records and to devise and maintain systems of internal accounting control.
  - The anti-bribery provisions prohibit any offer, payment, promise, or authorization to pay money or anything of value to any foreign official, political party, or candidate for public office, which is intended to influence any act or decision in order to assist in obtaining or retaining business.
  - The accounting provisions contain two subsections, termed the “books and records” and “internal controls” provisions.
    - Books/records: Issuers must “make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer.”
    - Internal controls: Issuers must “devise and maintain a system of internal accounting controls ...”

## Enforcement of FCPA

- Enforcement of the FCPA is divided between the U.S. Securities and Exchange Commission (SEC), which may enforce the civil provisions of the statute against issuers, and the U.S. Department of Justice (DOJ), which may enforce the criminal and civil components of the statute.
- Recently, the enforcement efforts are coordinated between the US and foreign officials, as most countries now have anti-corruption laws and the foreign countries can ride the coattails of U.S. enforcement agencies.

- “Business should be won or lost on the merits of a company’s products and services, not the amount of bribes paid to government officials. This indictment reflects our ***commitment to holding individuals, as well as companies, accountable*** for violations of the FCPA.”



*Assistant Attorney General Lanny Breuer on Siemens FCPA charges (December 2008)*

## Summary of 2012 FCPA Enforcement Activity

- 27 resolved cases by DOJ/SEC
  - 20 against companies
  - 7 against individuals
- Why so weighted towards companies?
  - Individuals litigate
  - Companies do not – cost is too high
    - Siemens: \$1.6 billion in penalties
      - Attorneys fees, investigative fees and consultant's fees were \$900 million
- 29 known investigations initiated
- 100 known pending investigations by DOJ/SEC



# Antitrust



## Summary of 2012 Criminal Antitrust Enforcement

- Over \$1 billion recovered by DOJ from criminal antitrust offenders in 2012
  - \$500 million fine imposed against AU Optronics Corporation
  - \$470 million fine imposed against Yazaki Corporation
- International cartel investigations
  - Auto parts (*e.g.*, Yazaki Corporation)
- Increased cooperation/coordination between DOJ and foreign authorities
- Increased enforcement activity by foreign authorities
  - EC: € 1.875 billion (\$2.45 billion)

# Money Laundering



## Recent Enforcement Actions

- HSBC
  - \$1.9 billion and Deferred Prosecution Agreement
- Other recent cases
  - Bank of Tokyo – \$250 million
  - Standard Chartered – \$250 million
  - ING Bank NV – \$619 million

## False Claims Act



## The False Claims Act

- The False Claims Act (31 USC § 3729) creates liability against any person who submits a false claim to the government
- Knowledge:
  - actual knowledge
  - deliberate ignorance
  - reckless disregard
- *Qui tam* provisions
  - Allows private persons to sue on the government's behalf
  - Relators are generally entitled to portion of any recovery as well as legal fees and expenses (15-25% when government intervenes and 25-30% when the government does not)

## The False Claims Act

- Substantial penalties
  - Treble damages (i.e., three times actual damages)
  - Fines of \$5,500 to \$11,000 for each false claim
- *Qui tam* actions are filed under seal, which triggers government investigation
- Government can either:
  - Intervene in the action (i.e., take over the case)
  - Decline to intervene, thus allowing the relator to proceed
    - By statute DOJ has 60 days to decide whether to intervene
    - By practice DOJ will continuously obtain *ex parte* extensions

## Summary of *Qui Tam*/False Claims Act Activity in 2012

- \$4.9 billion in settlements/judgments in 2012
  - \$3.3 billion came from *qui tam* suits
  - Health care: \$3 billion
  - Housing/mortgage fraud: \$1.4 billion
- 647 *qui tam* suits filed in 2012
- Numbers are staggering
  - GlaxoSmithKline: \$1.5 billion
  - Merck: \$441 million
- Plaintiffs are aggressive because the rewards are very high



## *Qui Tam*/False Claims Act: Emerging Areas of Risk

- Financial services industry – mortgage and securitization claims
- Customs related claims
- State *qui tam* case for taxes

## Data Breach

Pentagon will respond with force to cyber attacks...



## Data Breach

- SEC Guidance on Disclosures Regarding Cybersecurity Risks and Cyber Incidents (October 2011)
  - May 2013: Chairman White asks staff for briefing on past compliance and recommendations for further SEC action
- President Obama's Executive Order: "Improving Critical Infrastructure Cybersecurity" (February 2013)
- DOJ
  - FY 2014: \$92.6 million in program increases (\$668 million total)
- State Attorneys General
  - LivingSocial network breach: Connecticut and Maryland AGs requested information

## Multinational Investigations: Overview

- **Data and Documents**
  - Foreign Restrictions on Personal Data
  - Blocking Statutes
  - Electronic Evidence
  - How to Handle Foreign Evidence
- **Employee Interviews**
  - Employment and Privacy Laws
- **Governmental Requests for Information**
  - Inquiries from U.S. Authorities for Foreign-Based Evidence
  - Company Personnel Crossing the Border

## Multinational Investigations: Overview of Key Factors

- **Privilege Issues**
- **Practical concerns**
  - Cultural/legal differences
  - Logistical issues in retrieving documents/data & conducting interviews (Language/Location/Logistics)
  - Hobson's choice with auditors

## Data and Documents

- **Foreign Restrictions on Personal Data**
  - Data protection laws have been adopted in many countries and can restrict access during internal investigations. Knowing the local laws in this area is essential.
  - Data protection laws not only prevent companies from reviewing information or correspondence deemed “personal” without the employee’s consent but, in securing the employee’s consent, the company may be required to provide the employee access to the information and give the employee the opportunity to correct any inaccuracies.

## Data and Documents

- **Foreign Restrictions on Personal Data**
  - The European Union’s Data Protection Directive 95/46/EC is the primary legislation on data protection in Europe.
  - That directive gives “personal data” a broad definition, saying that it is data that “relate[s] to an identified person or identifiable natural person” who “can be identified, directly or indirectly,” by reference to an employment identification number or “to his physical, physiological, mental, economic, cultural, or social identity.”
  - The Directive (and similar European laws) also limits the permissible circumstances in which personal data can be collected and reviewed.

## Data and Documents

- **Blocking Statutes**

- Many countries have put blocking statutes in place, based on the view that attempts by the United States to compel their citizens to meet discovery demands is contrary to their sovereignty, customs and national interests.
- These blocking statutes impose civil and/or criminal sanctions on those who directly comply with discovery requests without going through the channels set forth in the Hague Convention.
- In the context of an internal investigation, a company that transports data to the United States for review likely makes the information subject to subpoena in a United States court – and risks civil/criminal sanctions in the event blocking statutes are in place.



## Data and Documents

- **Foreign Evidence**

- The first step in handling foreign evidence is to understand the relevant country's laws surrounding data and discovery. Consultation with local counsel with data privacy and similar experience is essential in this area.
- After documents have been processed, an investigation team may consider allowing employees to review the collected documents first and identify documents that they deem personal. This may take place either before or after search terms have been run. A preliminary review of employee documents may slow down the investigation at first, but may be a useful compromise if handling resistance from a works council or data protection authority.

## Digital Forensics

- Best practices for deploying digital forensics (“DF”):
  - Engage DF support during the investigation *planning* stage
    - The earlier DF becomes familiar with the facts and issues, the better DF can become a force multiplier for the investigative team
  - Ask DF two questions:
    - Can DF do “X” technical analysis?
    - What else can DF tell investigators about the device(s) at issue, *i.e.*, what other analyses can DF perform to further the investigation?
- Understand when either internal IT and/or when external DF resources cannot further the investigation

## Digital Forensics

- Assessing your DF capabilities before the need arises:
  - Does your DF resource (internal and/or external) have DF labs with dedicated DF personnel?
  - Does the DF resource follow FBI protocols for evidence handling and storage procedures?
  - Is the DF resource US-EU Safe Harbor certified?
  - Can the DF resource deploy mobile DF labs worldwide on short notice?

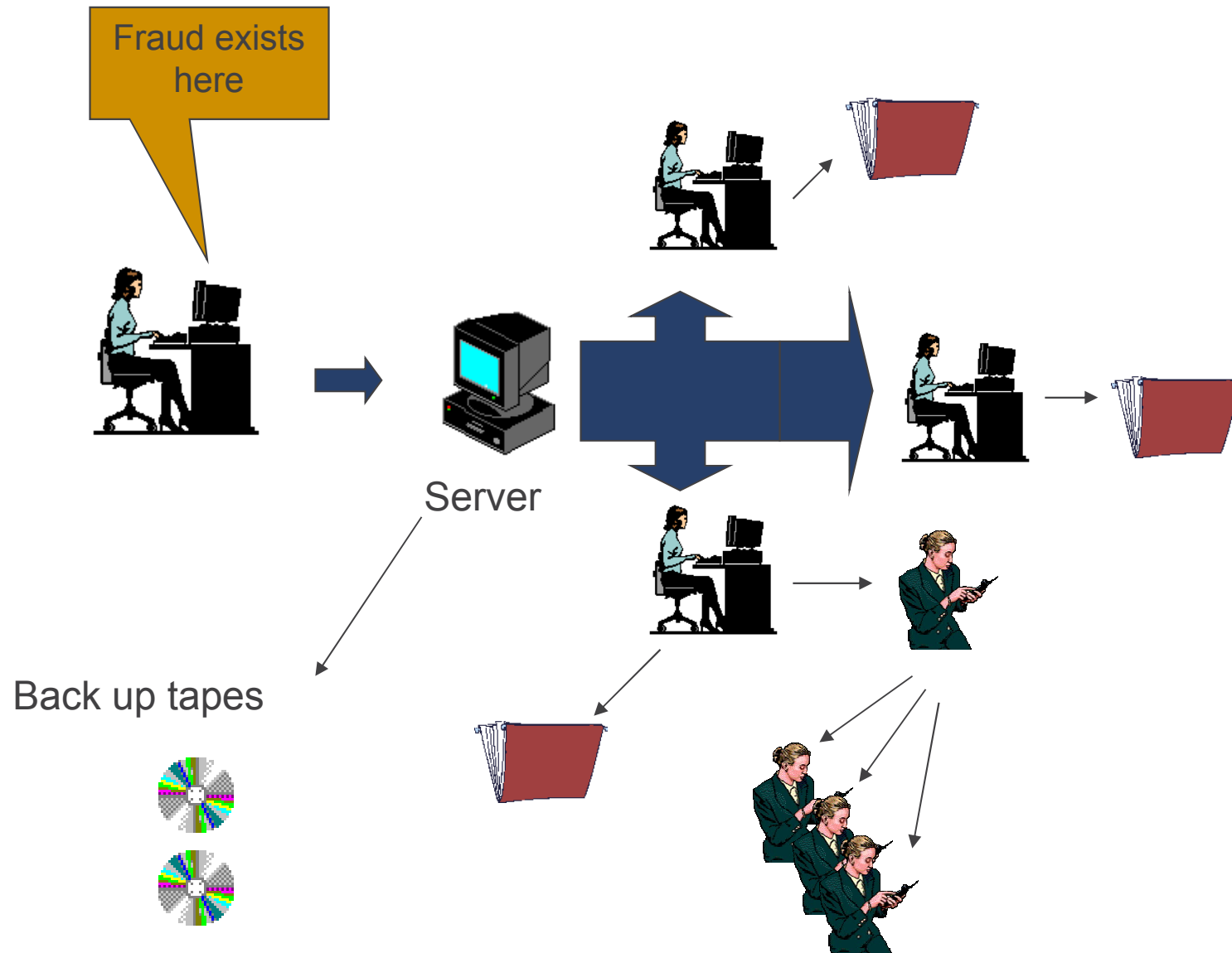
## Digital Forensics

- Indispensable investigative tool for today's world.
- Common issues DF can address:
  - Is a document authentic? When was it created?
  - Did a current or ex-employee steal trade secrets? e-mail sensitive company documents to an outside address?
  - How many credit card numbers did a hacker successfully access?
  - Did a witness spoliage digital evidence?
  - Did a user tamper with the content of an electronic document?
  - Who within the company is posting confidential corporate information in a web-based chat room?
  - Was a computer intentionally used to browse illicit images on the Internet?

## Digital Forensics


- DF identifies, preserves and analyzes data located on:
  - Laptops and desktops
  - in the cloud
  - portable devices
  - backup tapes
  - removable devices
  - file and e-mail servers/sharepoint


## Practical Example




## Practical Example

### Witness Interviews


1 creator = 

3 recipients = 

4 others = 

### ESI Collection

1 Original Computer = 

1 Server = 

3 recipients' computers = 

2 back up tapes = 

## Early Case Assessment Tools

- Investigation Centric attributes
  - Helps answer the who, what, where and when of an investigation
  - Speeds up the time to put a fence around an allegation after an investigation begins; critical in focusing attention on most fertile areas and individuals of an investigation; results in better communications within the organization about an investigation
  - Understanding the data to efficiently determine who is talking to whom, about what (*e.g.*, might be relevant that two people rarely speak but after one is interviewed there are 10 emails between them); also, a date range search can show the absence of email activity when it is expected to be present
  - Identifies code words and phrases or relevant unknown terms
  - Maps the frequency in which a term is discussed over a certain period of time (*e.g.*, “shred” after a legal hold is issued or subpoena is received)



## Employee Interviews

- The labor and employment laws of many foreign jurisdictions are protective of employees, and allow employees to refuse to submit to questioning by counsel conducting internal investigations.
- Privacy laws also may provide protections to employees that could excuse them from submitting to questioning by counsel.

## Governmental Requests for Foreign Evidence

- **Inquiries from U.S. Authorities for Foreign-Based Evidence**
  - The United States has entered into various Mutual Legal Assistance Treaties (MLATs) with other countries in order to assist one another in criminal enforcement investigations. Each specific MLAT defines the obligations of the countries to provide assistance and the scope of assistance. An MLAT may also contain evidentiary provisions that vary from the United States Federal Rules of Evidence.
  - Letters Rogatory are another method of obtaining foreign-based evidence. These requests flow through the federal courts to the courts of the foreign sovereign. As such, these requests are extremely time-consuming.

## Governmental Requests for Foreign Evidence

- ***SEC v. Deloitte Touche* (D.D.C. 2012)**
  - SEC served Deloitte with subpoena for documents abroad relating to Deloitte's audit of Chinese technology company
  - Deloitte argued that it cannot comply with the SEC subpoena because removing the requested documents from China would violate Chinese laws
- ***Catch 22***: Produce the requested documents and face the risk of penalties under foreign law, or withhold the requested documents and face possible contempt in the U.S.

## Governmental Requests for Information

- **Company Personnel Crossing the Border**
  - Border searches are an exception to the 4<sup>th</sup> Amendment, permitting searches of travelers entering and exiting the U.S.
  - The Department of Homeland Security released a statement outlining the numbers in more detail, confirming that, although the number is small, hundreds of computers are searched every year.
  - Most federal courts that have addressed the issue have concluded that searches of laptops, computer disks and other electronic storage devices fall under the border search exception, which means neither a warrant nor probable cause is necessary to support the search.

## Multinational Investigations: Privilege Issues

- It is well-established within the United States that the attorney-client privilege may apply to a corporation's internal investigation.
- However, in 1982, the European Court of Justice held that an EU rule of privilege, rather than a country-specific rule, applied in investigations into competition practices. This decision was the basis for later decisions that indicated that attorneys unlicensed within the EU may not enjoy privilege when working for clients within its jurisdiction.
- Further, communications from in-house counsel are treated differently in different countries, which should inform the extent to which in-house counsel assist outside counsel during the performance of an internal investigation involving activities outside the U.S.

## Hobson's Choice

- Waiver questions also arise with respect to requests by auditors. High-profile corporate scandals, the subsequent enactment of the Sarbanes-Oxley Act (SOX) of 2002, and other stringent regulations have resulted in increased liability, and therefore pressure, on outside auditors.
- Auditors now demand a much broader range and much more in-depth level of information from corporations and their investigative counsel. These requests frequently include the information obtained and work product created by legal counsel during internal investigations, despite the protections and privileges that can be afforded such information.

## Hobson's Choice

- The emergence of the globalization discussed earlier serves only to further muddy the waters on this question.
- With potential litigation/enforcement actions in so many different venues with so many different jurisdictional considerations, any determination of whether the release of information to auditors might result in a waiver is almost impossible to predict.

## Resolution & Settlement

- Resolution and/or settlement of global investigative matters have multiple factors to consider. It is similar to three-dimensional chess in that each action has multiple collateral consequences.





## Minimizing Risk of Enforcement Action

- Effective compliance and ethics programs
- Self-assessment/Risk profile
- “Tone at the top”
- Codes of conduct/Policies
- Procedures/Controls
- Training
- Audits
- Remediation

## 2012 DOJ/SEC FCPA Guidance

- “[B]oth DOJ and SEC place a high premium on self-reporting, along with cooperation and remedial efforts, in determining the appropriate resolution of FCPA matters.”
- Hallmarks of Effective Compliance
  - Commitment from senior management to a “culture of compliance” and a clearly articulated policy against corruption;
  - A code of conduct that is “clear, concise, and accessible to all employees and to those conducting business on the company’s behalf”;
  - An autonomous reporting structure bearing responsibility for oversight and implementation of the compliance program;

## 2012 DOJ/SEC FCPA Guidance

- Hallmarks of Effective Compliance (Cont.)
  - Appropriate assessment of risk and proportional devotion of compliance resources;
  - Positive incentives for corporate compliance and appropriate disciplinary measures;
  - Adequate due diligence in transactions with third parties;
  - Mechanisms for confidential reporting of potential violations within the company; and
  - Continuous development of the compliance program.

## Benefits of Strong Compliance

Congress of the United States  
House of Representatives  
Washington, DC 20515

January 10, 2013

Mr. Michael T. Duke  
Chief Executive Officer  
Wal-Mart Stores, Inc.  
702 SW 8th Street  
Bentonville, AR 72716

We are writing regarding new allegations that Wal-Mart systematically bribed officials throughout Mexico in order to evade zoning, environmental, and permitting laws at the company's Bodega Aurrera store in Teotihuacan, Mexico. We are concerned that your company's public statements that the company was unaware of the allegations appear to be inconsistent with documents we have obtained through our investigation. Contrary to Wal-Mart's public statements, the documents appear to show that you were personally advised of the allegations in October 2005.

and commerce."<sup>2</sup>

In response to this report, the New York Times reported that your company spokesman "said that while executives in the United States were aware of the furor in Teotihuacán they did not know about the corruption allegations."<sup>3</sup> However, documents obtained by our staffs from a confidential source indicate that you and other senior Wal-Mart officials were personally informed about these bribery allegations on multiple occasions.

<sup>1</sup> *The Bribery Aisle: How Wal-Mart Got Its Way in Mexico*, New York Times (Dec. 17, 2012) (online at [www.nytimes.com/2012/12/18/business/walmart-bribes-teotihuacan.html?ref=global-home&\\_r=1&](http://www.nytimes.com/2012/12/18/business/walmart-bribes-teotihuacan.html?ref=global-home&_r=1&)).

<sup>2</sup> *Id.*

<sup>3</sup> *Id.*

## Morgan Stanley Declination

"[C]onsidering... Morgan Stanley **constructed and maintained a system of internal controls, which provided reasonable assurances that its employees were not bribing government officials**, the [DOJ] declined to bring any enforcement action against Morgan Stanley related to [employee's] conduct. The company **voluntarily disclosed** this matter and has **cooperated throughout** the department's investigation."

4/25/12 DOJ Press Release

## Minimizing Risk in Cross-Border Investigations

- Boy Scout Motto: “Be Prepared”
  - Compliance/Policies/Training/Audit
  - Have an Investigations Protocol in Place
- Conducting the Investigation: Three-Dimensional Chess
  - Determining what happened
  - Privilege
  - Data Privacy/Blocking Statutes
  - Collateral consequences
    - Government enforcement/Multiple jurisdictions
    - Private suits
    - Disclosure obligations

## Conclusion

- As our economy becomes more global and the cross border operations of corporations expand, the complexities of multi-jurisdictional internal investigations increase. This is an area fraught with peril for the uninformed and unprepared. There are many difficult challenges and the risks are high.
- **Bottom Line**: The challenges and risks can be navigated, but it's a little like swimming with sharks – you must be VERY CAREFUL.

