Morgan Lewis

Foreign Corrupt Practices Act

A Focus on FCPA Investigations

presented by: **Leslie R. Caldwell**

Kelly Moore

Lisa Tenorio-Kutzkey

March 4, 2010

Today's Presenters

Leslie R. Caldwell
New York

Kelly Moore
New York

Lisa Tenorio-Kutzkey
San Francisco

Morgan Lewis

Topics of Discussion

- When is an FCPA investigation necessary?
- How much investigation is enough?
- What are the privacy challenges abroad?
- Interviews in international investigations
- Why and when to self-report?
- The importance of remediation
- Q&A

When Is an FCPA Investigation Necessary?

Are You Subject to the FCPA?

- "Issuers"
  - Any company whose equity or debt is traded on a U.S. exchange, including companies based overseas
  - Privately held companies who file regular reports with the SEC because, e.g., they issue debt to the investing public
- "Domestic Concerns"
  - Any entity that is organized under the laws of the United States or that has its principal place of business in the United States
- Any "person," including an organization, wherever located, that, while in the territory of the United States, does any act in furtherance of prohibited conduct

Compliance Programs

- Companies are expected by the U.S. government to have in place effective compliance and ethics programs
- To be effective, a compliance program must be designed to detect and prevent wrongdoing, and to address wrongdoing if it occurs
- All companies with overseas operations should have an anticorruption component to their general compliance programs
  - Anticorruption compliance should be tailored to the company's business
  - Anticorruption compliance should reflect level of anticorruption risk in countries where company has operations
  - Larger companies are expected to have more formal processes than smaller companies

Compliance Programs

- An effective anticorruption compliance program must include an ability to respond to and investigate credible allegations or evidence of misconduct
  - Necessary investigative capability varies with size of company and nature of its business
  - Large, multinational businesses may be expected to have in-house rapid response team
  - Smaller businesses may have more informal processes to conduct investigations

Credibility of Allegations

- When are allegations “credible” enough to warrant investigation?
- “Credible” allegations may arise from:
  - Compliance or other hotlines
  - Customers, business partners, competitors
  - Employees or former employees
  - Due diligence
  - Analysts and media
  - Investigation initiated by foreign government
  - Subpoenas or requests for information

Credibility of Allegations

- Some allegations will be too general or vague to warrant an investigation
  - Anonymous hotline report that “the sales team in China is corrupt”
- The more specific or serious the allegation, the more a failure to investigate will be susceptible to second-guessing
  - Anonymous hotline report that “the regional sales director in Kenya paid a bribe to get the Q3 provincial hydroelectric deal”
- Cannot fail to investigate simply based on the source’s general lack of credibility
  - Disgruntled former employee involved in litigation with company

How Much Investigation Is Enough?

How Much Investigation Is Enough?

- What is the nature of the allegation?
  - Specific misconduct directed by, known to, or condoned by executive-level management in the United States
  - Specific misconduct directed by, known to, or condoned by executive-level management in the country or geographic region
  - Specific misconduct by identified group of people
  - Specific misconduct in connection with particular transaction(s)
  - Unspecified misconduct by named group or individual
  - General allegation of misconduct with no detail

How Much Investigation Is Enough?

- Specific allegation of misconduct directed by, known to, or condoned by executive-level management in the United States
  - Make initial credibility determination
    - This may be done in-house
    - If allegation has credibility and is serious, a broader investigation must be conducted
  - Outside counsel likely will be needed; consider if firm should be "independent"
  - Audit/special committee of board of directors likely should supervise investigation

How Much Investigation Is Enough?

- Specific allegation of misconduct directed by, known to, or condoned by executive-level management in the country or geographic region
  - Outside counsel likely will be needed
    - Regular outside counsel likely can conduct investigation
    - Consider “independent” counsel if regular counsel has worked extensively with local management
  - Outside counsel can report to legal department or management
  - Legal department or management should report to board committee

How Much Investigation Is Enough?

- Allegations about specific lower-level individuals or groups, and general allegations
- In-house resources often may be used to conduct entire investigation
  - Investigation should be done under direction of the legal department
  - Electronic and other documentary evidence should be captured and preserved, as appropriate
  - Investigative steps and conclusions should be documented
  - Interviews and results of forensic or other analyses should be memorialized
  - If possible FCPA violation is found, consider retaining outside counsel to conduct further investigation

How Much Investigation Is Enough?

- How thorough must an FCPA investigation be?
  - Investigation must be thorough enough to determine the scope of improper conduct, identify those involved, and determine whether management personnel participated in, were aware of, or otherwise condoned the activity
  - Investigation must be able to withstand government scrutiny should the company decide to self-report, or should the government learn of the conduct in some other fashion

How Much Investigation Is Enough?

- Steps that must be included in an investigation:
  1. Preservation of relevant documents and electronic records
     - Should include at least first-level managers even if no allegations against them
     - Consider usefulness of document preservation notice
  2. Review of documents in custody of relevant individuals, including email
  3. Interviews of relevant people must be conducted and memorialized
  4. Investigative steps should be documented in detail
  5. Document factual conclusions
  6. Consider whether to document legal conclusions

How Much Investigation Is Enough?

- "Scoping" the investigation
  - Investigation may be limited to subject matter and geographic area at issue
- However, investigation must "follow the evidence;" if additional anticorruption issues are discovered, they must be investigated
  - Failure to do so will render the investigation incredible in the government's eyes
  - Company may need to conduct a new, even more expensive investigation under the government's direction

How Much Investigation Is Enough?

- When can a company stop investigating and remedy the problem?
  - Investigation must be thorough enough to determine the scope of improper conduct
    - Company cannot “refuse to know” about improper conduct
    - Difficult to remedy a problem before understanding its scope
  - Investigative steps needed will be driven by the facts and accompanying level of FCPA risk
    - Company learns that there is a pervasive practice in China of providing small gifts to customers, including government officials, during Chinese New Year
    - Company learns that for years its China subsidiary has been arranging and paying for overseas travel for customers who are employees of state-owned enterprises

How Much Investigation Is Enough?

- If an FCPA violation is discovered in one region of a particular country, must the investigation be expanded to the entire country or other countries?
  - Must consider quality of company's compliance and ethics program
  - Must consider actual culture of compliance
    - Did country or regional management participate, condone, or willfully blind themselves to improper activity?
    - Do those involved in the potential FCPA violation have duties and responsibilities in other areas?
    - Were those involved in the potential FCPA violation previously involved in other misconduct?
  - Must consider reliability of company's books and records and internal controls
  - Must consider risk profile of country or region

How Much Investigation Is Enough?

- How can a company limit investigative costs and maintain credibility?
- Depending on the facts:
  - Avoid “boiling the ocean” once the scope of a problem is known
  - Avoid looking for potential issues not suggested by the evidence
  - Consider whether processing, in addition to preserving, particular laptops and email accounts is necessary
  - Avoid unnecessary translations
  - Consider which interviews need to be formally memorialized
  - Consider form of final investigative report

What Are the Privacy Challenges Abroad?

Overview

- Privacy viewed as a fundamental right abroad
- Collecting, processing, and transferring personal data is prohibited by law in many foreign countries
- Several types of privacy challenges:
  - Data protection laws, which are focused on maintaining personal privacy
  - Blocking statutes, which are intended to prevent U.S.-style discovery
  - Government secrecy laws, which protect confidential government information and state secrets

Navigating the Process

- Investigations often require data collection in various jurisdictions
- Key is to map out a plan:

Step 1:	Identify relevant laws
Step 2:	Consider consent
Step 3:	Evaluate strategy
Step 4:	Minimize the risk

Step 1

- Identify applicable jurisdictions:
  - Where are the relevant employees based?
  - What are their nationalities?
  - Where is the relevant entity based?
  - What categories of data are required?
  - Where is that data stored?
  - From where is it accessible?
- Identify applicable laws and relevant restrictions on data collection, processing, and transfer

European Union

- In Europe, primary concern is the EU Data Protection Directive
  - Protects “fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data”
  - Applies to workplace communications and documents
- Member states may also have additional data protection laws

European Union

- EU Directive prohibits “processing” and transfer of “personal data” to any non-EU jurisdiction that does not apply “adequate” privacy protections
- Processing
  - Includes any “operation” performed on personal data
  - Examples include “collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction”

European Union

- Personal data
  - Broadly defined to include “any information relating to an identified or identifiable natural person”
  - Includes content (such as author, signature block, and meeting attendee list), IP or email addresses, and metadata
  - Heightened protections for sensitive personal data, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, or sex life
    - May be an issue with HR records

European Union

- Adequate protections
  - United States does not provide “adequate privacy protection”
  - Transfers are permissible under Safe Harbor Program, if U.S. companies can certify that they provide a certain level of data privacy and security in exchange for being deemed “adequate” under the EU Directive
  - Transfers also are permissible when “legally required on important public interest grounds or for the establishment, exercise or defense of legal claims”
    - Issue if U.S. subpoenas qualify

Step 2

- Consider if you already have consent
- Review company policies:
  - Have employees agreed in writing to limit use of computers, email, and handheld devices to business only?
  - Have employees agreed in writing to data collection in connection with an internal or government investigation?
  - Have employees agreed not to maintain confidential government information?
- Evaluate if this consent is valid in the relevant jurisdictions

Consent

- Ideally, consent should be:
  - In writing
  - Available in English and local language(s)
  - Signed before the data transfer
  - Clearly indicative of the purpose of the collection, what will be done with the information, and where it will end up
- In some jurisdictions, may need consent of the responsible entity

Step 3

- Once you understand the applicable laws and availability of consent, then formulate the strategy
- Must consider:
  - Volume and location of the data
  - Urgency of review
  - Other factors

Strategy

- Other factors
  - Burdensomeness of full compliance
  - Ability to fully comply with requirements
  - Risk of noncompliance with laws
  - Likelihood of enforcement in relevant jurisdictions
  - Likelihood of disclosure by an employee
  - Need to conduct covert investigation
  - Document destruction concerns

Step 4

- Considerations to minimize risk:
  - Process and search data in local jurisdiction
  - Enroll in the Safe Harbor Program
  - Obtain employee and entity consent
  - Consider if illegal under local laws
  - Redraft company policies to provide consent

Interviews in International Investigations

Background

- Most effective way to conduct relevant information is to conduct witness interviews
- Primary goals:
  - Gather relevant facts
  - Understand or clarify documents
  - Assess credibility
  - Uncover the truth

Interview Considerations

- Once the decision to interview an employee has been made, must carefully consider the following:
  - When should the interview take place?
  - Why is this person being interviewed?
  - How should the interview be conducted?
  - Where should the interview occur?
  - Who should conduct the interview?
  - What should the interviewee be told?
  - How do you question a witness?
  - What documents should be used?

Interview Considerations

- When should the interview take place?
  - It depends
    - Quickly after discovery
    - After lower-level or less culpable interviews
    - After documents are reviewed
    - When available
  - Consider seriousness of allegations, potential pervasiveness of conduct, time in business cycle, any involvement by government

Interview Considerations

- Why interview this person?
  - What is his or her role in the investigation?
  - What information is he or she likely to provide?
- How should interview be conducted?
  - Critical that interviews are face to face, particularly in foreign countries
  - Exception for nonessential, clearly nonculpable, or otherwise unavailable witnesses

Interview Considerations

- Where should interview occur?
  - Neutral and private room away from observation
  - Consider hotel conference room
  - Be thoughtful of layout and availability of water and coffee
- Who should conduct interview?
  - One person, with second person to take notes
  - Lay out ground rules with translator
- What should he or she be told?

Interview Considerations

- How do you question a witness?
  - Consider your style, who you are, and how you appear
  - Consider age, cultural differences, and sophistication of witness
  - Different approach depending on witness's role in investigation
- What documents should be used?
  - What documents are relevant?
  - Before selecting a document, ask (1) What is the purpose? (2) Can the witness provide nonobvious information? and (3) Will it refresh a witness's recollection?

Why and When to Self-Report?

Affirmative Obligations to Report

- Nothing in the FCPA requires self-reporting of violations; **however**, other statutes/laws may give rise to an obligation to report
- Companies subject to SEC reporting requirements
  - Securities Exchange Act: Disclosure of Material Events
    - Quantitative or qualitative materiality
  - Sarbanes-Oxley Act of 2002
    - SOX §§ 302(a)(6), 404(a): Annual filings must include a report on the "effectiveness" of internal controls, including significant changes and corrective action re: deficiencies and material weaknesses
    - SOX §§ 302(a)(2), 302(a)(3): CEO and CFO must certify that the company's SEC reports do not contain any untrue statement of material fact or omit any material fact and fairly present the financial condition and operations of the company
  - Mergers and Acquisitions
    - Titan Report (SEC Section 21(a) Report, Rel. No. 51283, Mar. 2005)

Affirmative Obligations to Report

- Government contractors
  - Contractor Code of Business Ethics and Conduct of the Federal Acquisition Regulations (FAR)
    - A federal contractor is at risk of suspension or debarment for knowing failure to disclose criminal violations to the government when it has "credible evidence" of violations of federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 of the United States Code.
- Companies receiving TARP funds
  - Troubled Assets Relief Program (TARP)
    - Affirmative obligation to disclose "any credible evidence" that "a management official, employee, or contractor" has committed a violation of various criminal provisions.

FCPA Voluntary Disclosures

- In recent years, there have been hundreds of self-reports by companies regarding FCPA violations. **Why?**
- Possible benefits:
  - Principles of Federal Prosecution of Business Organizations – "Timely and voluntary" disclosure and cooperation with government is one of nine factors relevant to leniency/lower penalties
    - SEC Guidelines also encourage and reward voluntary disclosure
  - Federal Sentencing Guidelines Section 8C2.5(f)(1)(2) – Reduction in culpability score for effective compliance program, but not if conduct was not self-reported

FCPA Voluntary Disclosures

- Possible benefits
  - Former Assistant Attorney General Alice Fisher: “Voluntary disclosure followed by extraordinary cooperation with the Department results in real, tangible benefits to the company”
  - Current Assistant Attorney General Lanny Breuer: Companies will receive “meaningful credit” if they voluntarily disclose a violation, cooperate with DOJ’s investigation, and take remedial measures to ensure that the conduct resulting in the violation does not recur

FCPA Voluntary Disclosures

- Fear of independent DOJ or SEC discovery
  - Significant increase in resources devoted to investigating FCPA violations, including an entire new dedicated FBI squad
  - Industrywide investigations
  - Heightened awareness of FCPA due to increasing number of cases and large fines
  - Increasing likelihood of whistleblower disclosures directly to government

The Debate: Do the Benefits of Self-Reporting Outweigh the Risks?

- How great is the benefit?
  - No clear policy setting forth the specific benefits of self-reporting
  - Other factors—cooperation, remediation, effective compliance programs, nature/degree of misconduct, and senior management involvement—may play a greater role in whether the company is prosecuted or sued and any penalty is assessed
  - Lack of publicly available information about benefits to companies that self-reported

Self-Reports and Resolutions

- **Dow Chemical Company**
  - Conduct: $200K in multiple payments by Dow's subsidiary to different Indian government officials (business, tax, customs officials)
  - Settled with an SEC enforcement action and $325K civil penalty for violation of books and records provisions; cease and desist order
  - No DOJ criminal case against the company or others (payments made without approval or knowledge of any Dow employees)

Self-Reports and Resolutions

- **Control Components, Inc. (U.S. Co.)**
  - Conduct: $4.9M in improper payments related to government contracts ($31M in profits); $1.9M improper payments related to private contracts ($14.8M in profits); Improper conduct directed by senior management over 10-year period
  - DOJ resolution: Guilty plea to three counts; independent monitor; $18M fine (downward departure from guidelines of $27M-$55M)
  - Sentencing memo seeking downward departure emphasizes voluntary disclosure, cooperation, internal investigation, and remediation

Self-Reports and Resolutions

- **Schnitzer Steel**
  - Conduct: $1.8M in improper payments through wholly owned subsidiary (SSI Korea); profits of $61M
  - Resolution:
    - DOJ: Three-year DPA for Schnitzer Steel with independent monitor; guilty plea by subsidiary; $7.5M criminal fine for subsidiary
    - SEC: $7.7M disgorgement and cease and desist order
  - Fisher: "well below what it otherwise would have received"

Risks of Self-Reporting

- Near certainty of DOJ or SEC resolution/penalty
  - Likely DOJ resolution to include DPA, criminal plea, or nonprosecution agreement and criminal fines
  - Likely SEC resolution to include disgorgement and cease and desist order
- Loss of control of investigation and expansion into other areas
- Imposition of outside monitor may be costly and disruptive
- Potential for recidivist treatment
- Exposure to action by foreign governments/World Bank
- Exposure to related civil litigation
- Possible prosecution of individual employees

Factors to Consider

- Whether self-reporting is required
- Likelihood of independent discovery
- Nature of violation and strength of evidence
- Possible time-sensitive need to resolve FCPA exposure for merger
- Possibility of greater leniency by DOJ and SEC
- Risks outlined above

The Importance of Remediation

Importance of Remediation

- Principles of Federal Prosecution of Business Organizations:
  - "In conducting an investigation, determining whether to bring charges, and negotiating plea or other agreements, prosecutors should consider the following factors in reaching a decision as to the proper treatment of a corporate target: . . .

    The corporation's remedial actions, including any efforts to implement an effective corporate compliance program or to improve an existing one, to replace responsible management, to discipline or terminate wrongdoers, to pay restitution and to cooperate with the relevant government agencies."
- SEC policy also considers remediation

The Importance of Remediation

- Heart of an effective compliance program:
  - Tone at the top
  - Corporate culture
  - Employee incentives to report wrongdoing
  - Completeness/thoroughness of internal investigations

Remediation: Compliance Program

- Implement or update compliance program
  - CCO reporting to board of directors/audit committee
  - Risk assessments
  - Code of conduct for employees
  - Hotlines/mechanisms to report and receive allegations
  - Internal investigations
  - Training
  - Business standards and ethical standards for business partners
  - Third-party due diligence
  - Review/revision of third-party contracts (contractual right to audit their books)
  - Periodic compliance audits

Remediation: Employees

- Discipline and terminate wrongdoers
  - Consider what employment action is appropriate
    - Termination
    - Various forms of discipline
  - Discipline/terminate employees with knowledge of or involvement in FCPA violations
  - Discipline/terminate managers responsible for supervision/training of bad employees
  - Importance of consistency in employment actions
  - Avoid retaliation against whistleblowers or those who report misconduct

Remediation: Employees

- Training and communication:
  - Implement or update mandatory training on FCPA for all employees whose duties/responsibilities could enable them to violate the FCPA
    - In-person training
    - Webcasts/online training
    - Paper training
  - Training to include FCPA, approval process, revenue recognition, deal management and documentation, gifts and entertainment, reporting of wrongdoing

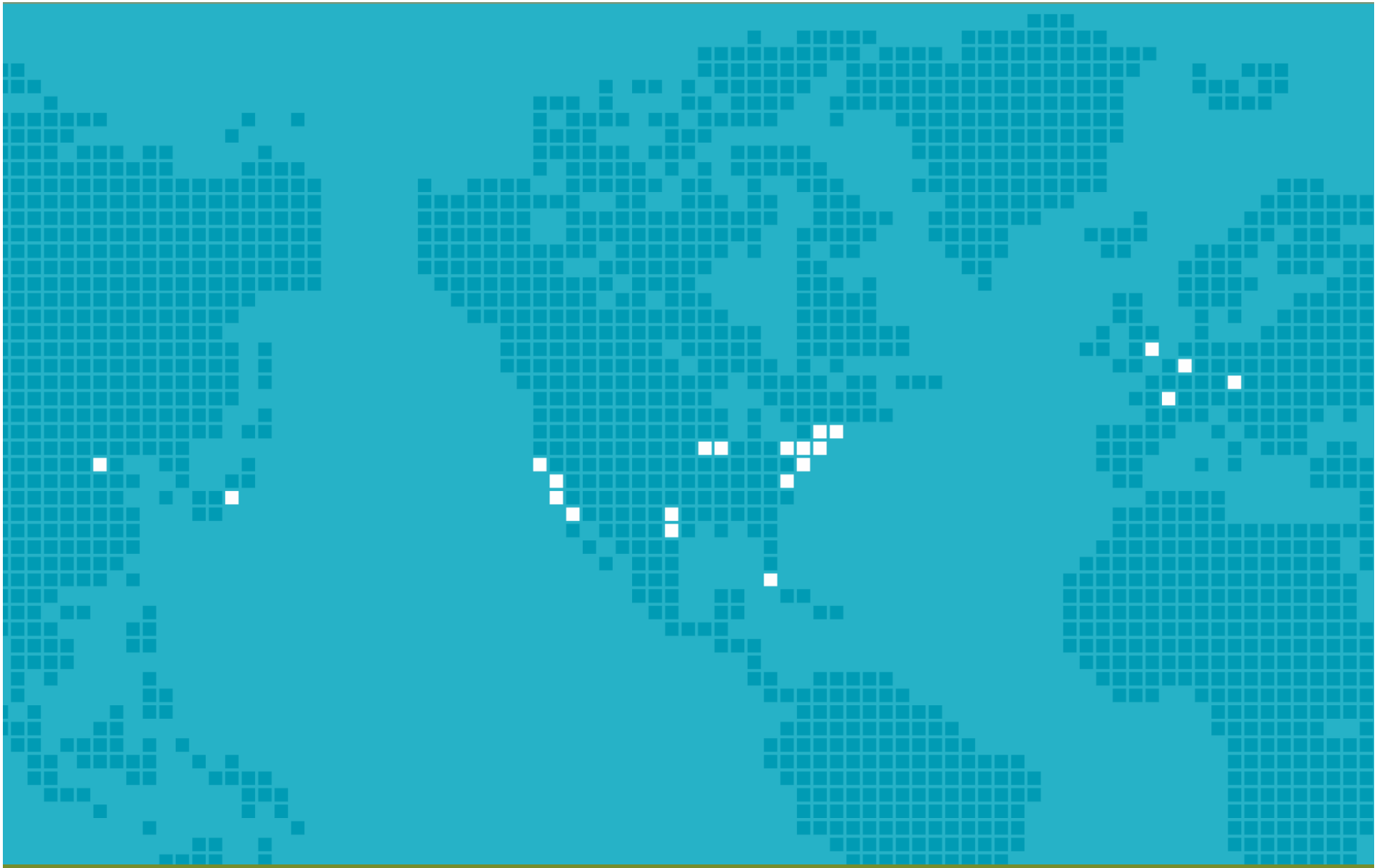
Remediation: Third Parties

- Terminate relationships with bad business partners
- Review contracts/agency agreements to ensure inclusion of antibribery provisions and auditing rights
- Conduct due diligence on third parties and business partners
- Audit third parties/business partners

Remediation: Internal Controls

- Review existing controls to make upgrades necessary to minimize risk of future FCPA violations

Q&A



worldwide

Beijing Boston Brussels Chicago Dallas Frankfurt Harrisburg Houston
Irvine London Los Angeles Miami Minneapolis New York Palo Alto Paris
Philadelphia Pittsburgh Princeton San Francisco Tokyo Washington