Part 4 in a Series

PUTTING IT ALL TOGETHER:
A "Do It Yourself" Guide for Building an FCPA Compliance Program

John W. Brooks
Senior International Counsel
619.699.2410
jwbrooks@luce.com
www.luce.com/johnwbrooks

SUMMARY

As reported in Parts 1-3 of this Series over the last three months, the Securities and Exchange Commission (SEC) and the Department of Justice (DOJ) have stepped up U.S. government enforcement of the Foreign Corrupt Practices Act, and the British Parliament has enacted the U.K. Bribery Act that will impose even tougher regulations on some U.S. companies. The U.S. government wants your company to have a "robust and effective" compliance program, while the Serious Fraud Office of the British government wants your company to have "adequate procedures" in place to detect corrupt activities. For the many companies subject to **both** sets of regulations, it's important to know the difference. This final Part of the Series lays out the basic building blocks of an effective FCPA compliance program, based on recognized *best practices*, no matter where in the world your company does business.

Best Practices You Say? Sez Who?

Lots has been written about what should be included in a robust and effective FCPA compliance program, but I think the place to go for the straight scoop may be the DOJ itself. Its *corporate compliance program guidelines* (imposed in settlement agreements with companies that have already been caught cheating) can be considered the current *gold standard* of **the minimum compliance program** the U.S. government expects you to have. So this should be your starting point.

- **COMMITMENT. The anti-corruption tone in your company needs to be set and supported at the top.** That means "senior management level." This commitment should be reflected in a written and highly-visible policy on compliance with *all* anti-corruption laws.

- **RISK ASSESSMENT. One size does not fit all.** Company A that peddles security equipment to government agencies in Africa will have a different risk profile from Company B that sells children's toys in Sweden. Company C that manufactures in several countries and distributes through business partners and agents in Indonesia will have a different set of problems than Company D that sells only online from Omaha. You get the idea.

- **CONTENT. Don't skimp on the detail.** A sanctimonious statement from the Board that your company is committed to "ethical behavior in all we do" won't cut it. What you should aim for are specific policies on every one of the "corruption hazards" your risk assessment has uncovered. If your salespeople take customers out to dinner or the theater, you will need a hospitality and entertainment policy. It should establish the limits on what your employees or agents can do in this regard and the penalties (immediate discharge comes to mind) if the limits are violated. Similar specifics should be included for *all the kinds of soft payments* your risk assessment indicates might conceivably take place. These include business gifts, political contributions, sponsorships, customer travel expenses, family favors (including scholarships for "Junior"), charitable contributions, tickets to the World Cup, and that old standby *facilitation payments* (more about this one later).

PUTTING IT ALL TOGETHER:
A "Do It Yourself" Guide for Building an FCPA Compliance Program

Part 4 in a Series

- **OVERSIGHT. Who will be making sure your program operates the way it should?** It needs to be someone from senior management who will have 1) specific reporting obligations to an independent monitoring committee established for this purpose, as well as 2) direct and unrestricted access to that committee, the audit committee, and the Board itself. Internal controls should also be established (particularly important for SEC reporting companies) to assure its financial books and records don't conceal illegal payments or "slush funds" for corrupt purposes.

- **TRAINING. Too many companies are content with "paper programs," that just sit in a drawer or stare blankly from their websites.** Real compliance programs (*robust and effective ones*) require extensive training at the front end and periodically afterward. This training should encompass everyone: officers, directors, employees, and - in some scenarios - agents and business partners as well, with specific emphasis on operations in high risk countries. The training should be repeated as necessary to reflect changes in the law and to address company-specific issues identified in prior periods. Graduates of periodic training programs can receive "compliance certifications" that can be made a prerequisite to holding certain positions within the company both domestically and abroad.

- **COMMUNICATION AND ACTION. Once you've built the foundations of a program, it's got to be allowed to operate efficiently.** This means the internal processes for 1) giving guidance and advice to officers, directors and employees, combined with *country or region specific* guidance to overseas agents and business partners; 2) providing incentives to employees to act in accordance with the program, 3) allowing confidential reporting of suspected compliance program violations, with assurance of anonymity, if requested, for the reporting person, 4) responding quickly and effectively to reports of suspected violations, and 5) imposing appropriate sanctions on violators.

- **DUE DILIGENCE AND CONTRACTS. Business partners (particularly smaller ones), as well as *all* agents and consultants, need to be vetted.** The adage "he who sleeps with dogs wakes up with fleas" should be your marching song! Due diligence in choosing your joint venture partners, distributors, agents, and consultants is time-consuming, but vital. Your own government, through its overseas consular offices, may be a source of interesting and useful information about the people or companies you're thinking about going into business with. Local banks and accounting firms are another potential source. Once your potential new partner has passed all due diligence tests, it's time for a meeting to discuss his or its business and ethical obligations and incorporate them in a comprehensive contract requiring regular detailed reports and at least annual certifications of compliance.

- **REVIEW AND EVALUATION. Practice won't make perfect in the area of squelching corruption, but it'll help.** The senior management guy you appointed to run your program (see "Oversight" above) should be required to advise the Board and its Audit Committee periodically on whether the program is working the way it was designed to work, and his or her full monitoring committee should present at least an annual evaluation of its efficacy and how it might be improved.

Will All of This Keep You Out of Jail?

Probably not, but the DOJ may give you "compliance credit" for having a robust and effective program in place *if the following are also true*:

- **The program you've now established detects the corrupt act before it becomes known, or likely to be discovered, outside your company.**

- **You promptly "self-report" the corrupt act to the proper governmental authority.**

- **And, nobody with operational responsibility for your program can have participated in, condoned, or willfully ignored the corrupt act.**

PUTTING IT ALL TOGETHER:
A "Do It Yourself" Guide for Building an FCPA Compliance Program

Part 4 in a Series

OK, Tell Me That's Enough to Obtain Leniency From the Government?

Sorry, I can't. If you really want to become *bulletproof*, you might also consider doing this:

- Having your compliance activities of the last several years reviewed by a major accredited outside review firm and disclosing the results of that review to the DOJ, the SEC - and publically.
- If the review turns up corrupt acts, taking appropriate ameliorative measures and submit to another five year review to make sure those measures worked.
- Hiring a full-time professional *FCPA compliance officer* to certify your compliance annually to relevant government agencies.

You Said You Were Going to Come Back to "Facilitation Payments."

The FCPA isn't the only anti-corruption law in the world, but it's the only one I know that still condones "facilitation payments." If your company has a business presence in the United Kingdom (and that's a lot broader than just the country of England itself), it will be subject to the U.K. Bribery Act (recently announced now to come into effect sometime this summer), and under it facilitation payments (or "grease payments" as they're sometimes called) are absolutely prohibited. Rather than requiring your employees to take Remedial Geography 101 as to the extent of the "United Kingdom," give serious consideration to eliminating the FCPA facilitation payment exception from your program altogether.

More Information.

For more information about the FCPA and how to create an effective FCPA Compliance Program for your company, contact your principal Luce Forward lawyer or the author of this Series at jwbrooks@luce.com. A printer-friendly PDF version of the previous three Parts follows.

Getting Caught With Your FCPA Pants Down - What To Do When the Phone Rings

Part 3 in a Series

John W. Brooks
Senior International Counsel
619.699.2410
jwbrooks@luce.com
www.luce.com/johnwbrooks

SUMMARY

As reported in Parts 1 and 2 of this Series over the last two months, the Securities and Exchange Commission (SEC) and the Department of Justice (DoJ) are stepping up government enforcement of the law known as the "Foreign Corrupt Practices Act." If your company does business overseas - particularly in some of the high risk countries - the chances of an unlawful payment being made are higher than you may want to admit. And if a payment that's prohibited by the FCPA is made, the chances of it coming to the attention of a third party is almost guaranteed. Once that happens, someone will be calling you. **What do you do then?**

Scenario One: The Company Finds its Own Violation.

If you already have an FCPA corporate compliance program ("Program") in place, assume your company's ombudsman learns - or your Program hotline is told - that a violation has taken place. If you don't already have a Program in place, simply assume a recent rumor has been confirmed. What do you do? Self-report or hope no one else finds out? **Here are some of the considerations:**

- Who else knows? Have you discussed the ***alleged violation (AV)*** with your Board yet?
- Have you taken any ***remedial action*** yet or do you plan to do so?
- How serious is the ***AV*** (number of people involved, their position(s) in the company, strict or vicarious liability standards if prosecuted) and what kind of ***reputational damage*** will your company suffer if (when) it comes to light?
- If you have a Program in place, does it measure up to the government's standards for ***compliance credit***?
- What are the chances a disgruntled employee or some other ***whistleblower*** will turn you in if you don't beat him to it?
- Does your company do business with, in, or from the U.K., thereby perhaps involving the ***U.K Bribery Act*** as well?

Scenario Two: The Government Finds Your Violation.

The phone rings. It's for you, and it's the DoJ. Oops! Whether you already have a Program in place or not, most likely you're toast, and your job will be to keep the toast from burning to a crisp! If you have a "qualifying" Program up and running, you may be able to hold down the penalties. If you don't, you may as well just go quietly. **Here are some things to consider:**

- How ***robust and effective*** is your Program. Would its ***strength of design*** and ***effectiveness of operation*** been likely, sooner rather than later, to have uncovered the ***AV***? If the U.K. Bribery Act is involved, do you believe your Program meets the U.K. standard of ***"Adequate Procedures"***? Did a ***"Senior Officer"*** of your company have secret knowledge of the ***AV***?
- Does your Program qualify under the U.S. Sentencing Commission's requirements for receipt of ***"compliance and ethics program credit"***?

Getting Caught With Your FCPA Pants Down - What To Do When the Phone Rings

Part 3 in a Series

- What was the relationship between your company and the alleged violator? Is he or she an ***employee*** or an ***agent***? Is the potential liability ***strict*** or ***vicarious***?

- If your company had already discovered the ***AV*** by itself, what action(s) had you already taken to ***advise the Board, re-examine and possibly strengthen your Program, and re-train, terminate or otherwise sanction the alleged violator(s)***?

- What ***changes in your manner of conducting international business*** are you willing to agree to with the government? A major international company recently shut down operations in three notably corrupt countries because it concluded it couldn't continue to do business in those places and still comply with the FCPA!

- Are you ***willing to cooperate*** in the government's investigation in the hope of a ***reduced sanction***?

- What ***additional costs*** (financial and reputational) ***are you willing to incur*** by refusing to cooperate with the government in its investigation?

Scenario 3: A Whistleblower Turns You In.

"Whistleblowers" come in at least two *not so tasty* flavors: **first,** the ***bounty hunter*** and **second**, the ***shake-down artist***. The U.S. Government has created the first in the Dodd-Frank bill. Self-interest has created the second. The first operates under the legal imprimatur of Congress; the second operates from the proverbial "darkened phone booth." They need to be treated differently, but it's not hard to tell them apart. **Here are some thoughts on this troubling topic:**

- The ***first type*** is entitled, under the right circumstances, to ten to thirty percent of all fines in the amount of $1 Million or more ultimately collected from you by the U.S. Government for relevant, accurate, and useful information about an ***AV*** furnished by him or her to the DoJ - not only from the originally reported ***AV***, but from any related action(s) that may be brought by other state or federal enforcement agencies later on. Fines in the last two years were in the range of $2 billion and the prospects for increased fines, along with longer jail terms, are rising.

- The ***second type*** is not entitled to anything, but could be more problematic than the first.. He or she is likely to use a pseudonym and request that any **silence buying payment** be kept strictly in confidence. One of your concerns needs to be that this shake-down artist may have a connection with your company - perhaps even an employee. The two most likely reasons this person is not talking to your company ombudsman or using your Program hotline are either 1) your company ***doesn't have a Program***, or 2) your Program provides no ***"payoff"*** beyond a favorable mention in the monthly employee newsletter.

- ***What can you do in the first situation?*** Not much. You may not even know this person exists until his or her information causes the commencement of a governmental investigation. In the past, by and large, whistleblowers have been civic minded citizens, along with some disgruntled employees, ex-spouses, and activists of various stripes, either doing their duty as they saw it, seeking revenge for perceived injustices, or looking for a small payday. But with Dodd-Frank, *no more small paydays*! The legislation may have triggered a ***new growth industry***, and this, of course, can lead to a vexatious and expensive problem, particularly if the allegation that is made to the government in ***a shot at the brass ring*** is (1) untrue, (2) only partially-true, or (3) could easily have been remediated if communicated to you pursuant to a properly functioning Program.

- ***What can you do in the second situation?*** First off, ***all silence buying payments should be off the table***. But finding out the relationship of this person to your company and his or her motivation might be a ***first order of business***. If you have a Program, perhaps this person can be convinced to step inside the Program and receive recognition for his or her cooperation in the remediation of the ***AV***. The chances of this, of course, are significantly greater if the recognition your Program provides has a ***monetary element***. If you ***don't*** have a Program, consider whether this would be shakedown artist might be a good recruit for the group you'll need to put together to help your company develop a ***robust and effective*** Program - and paying the new recruit for services rendered!

Getting Caught With Your FCPA Pants Down - What To Do When the Phone Rings

Part 3 in a Series

As you can see right away, your options in dealing with whistleblowers are limited if you don't have an up and running Program. Less than two months ago (November 19, 2010), the DoJ announced a new era of aggressive FCPA enforcement and warned that you should not wait for the DoJ to "come knocking." Prudent executives will probably find this ***reason enough*** to have or to create a Program that meets the government's recommended standard as set out in the OECD's "Good Practice Guidance on Internal Controls, Ethics, and Compliance." This Guidance includes:

- ***Assessing your company's individual corruption risks***, such as industry and geography, to custom tailor your internal controls, ethics, and compliance programs.
- ***Implementing a clear and visible anti-corruption policy*** strongly supported by senior management and applicable to all employees and entities your company controls. Areas of high risk, such as gifts and hospitality should receive special attention.
- ***Appointing an adequately-resourced and fully-autonomous senior corporate officer*** to oversee your Program and giving that person the responsibility and authority to report directly to the Board.
- ***Making prompt advice available to all employees and business partners*** with compliance questions, particularly guidance on transactions involving foreign jurisdictions.
- ***Providing a prompt and confidential reporting mechanism*** for all employees and business partners and protecting them from any sort of retaliation.
- ***Reviewing and re-assessing your program regularly*** both to improve its operational efficiency and to adapt it to new business vectors.

In recognition of such a Program - and your voluntary cooperation in any investigation - your government says it might be inclined to go easier on you and your company than it otherwise would. Consider whether these are words it's come time to heed!

Coming Next.

Next month, Part 4 (the final part) of this Series will describe in greater detail just how to establish the kind of Program that prudent companies are realizing is an important risk management tool - and useful for keeping their execs out of jail, as well.

More Information.

For more information about the FCPA and how to create an effective FCPA Compliance Program for your company, please phone your principal Luce Forward lawyer or contact the author of this article at jwbrooks@luce.com. Keep reading for a copy of last month's article on your company's vicarious FCPA liability for the actions of people you might not even know (and Part 1 as well).

The U.S. Government Expects You to Be "Your Brother's Keeper" - And If You Fail, It Can Fine You and Send You to Jail for *Something Someone Else Did!*

Part 2 in a Series

John W. Brooks
Senior International Counsel
619.699.2410
jwbrooks@luce.com
www.luce.com/johnwbrooks

More Information.

For more information about the FCPA and how to create an effective FCPA Compliance Program for your company, please phone your principal Luce Forward lawyer or contact the author of this article at jwbrooks@luce.com. Last month's article on FCPA basics, follows this e-Update.

SUMMARY

As reported in Part 1 of this series last month, the Securities and Exchange Commission (SEC) and the Department of Justice (DoJ) are stepping up government enforcement of the law known as the "Foreign Corrupt Practices Act." One of the government's most fertile fields for finding FCPA violations is in the far away overseas parts of your business - and it involves what your partners, agents and consultants are doing in those places. You may be tempted to respond "I can't control their every action." And that may be true. But your government says it doesn't care, and you may still be in trouble.

Strict or Vicarious? What's the Difference?

If one of your **company's employees** commits an FCPA violation, your company is strictly liable - that means it has no defenses - under an ancient legal theory called *respondeat superior*. But if one of your company's **business partners, agents, or consultants** steps over the FCPA line (intentionally or unintentionally), a different theory of liability comes into play called ***vicarious liability***, but the result can be the same. Why? Because it's the government's position that your responsibilities extend beyond your own company and its employees to include the conduct of certain third parties, such as your joint venture partners, sales agents, subcontractors, distributors - and that often ambiguous and hard to classify figure, the **overseas consultant**. The government says you can't ignore signs these ***"business partners"*** of yours may be violating the FCPA, because, it argues, you're the one that put them in a position that was conducive to FCPA violations in the first place.

A Longish - But Perhaps Useful - Example to Illustrate a Basic Point

Let's say you're a C-Level officer of a large U.S. medical products company, and you're in ***acquisition mode***. Your acquisition target is a UK medical devices company ("StentsRUs") with a hot new model that would fit perfectly into your product line. Some time ago Stents had hired an Indian consultant named Gupta who advised contracting with a well-known Indian distribution company ("HinduMed") to handle Stent's sales in the Indian market. HinduMed's management was Western-trained (mostly 'MIT PhDs') and very entrepreneurial. Stents has a business plan for India that gives first year discounts to HinduMed in order to stimulate first year purchases. One might think, "Basic Marketing 101," right?

But what you don't know is that HinduMed had conceived a plan to convert this ***manufacturer's discount*** program into an ***agent's commission*** program for local public and private hospital managers, offering to pay those managers the discount money as a commission for recommending the purchase of Stent's hot new product. The commission program - no surprise - is a roaring success, and HinduMed's sales were going through the roof when one of its employees, mad about something, tips the payments to the British Serious Fraud Office (a UK analog to the US DoJ). While the SFO investigation is going on, an Indian Customs Officer requests a small payment from consultant Gupta to speed up the clearance of Stents' medical devices through Indian Customs. Gupta makes the payment, but is annoyed and emails Stents' VP Sales requesting reimbursement. The VP Sales at that very moment happens to be having dinner in Shanghai with a PRC government hospital administrator

The U.S. Government Expects You to Be "Your Brother's Keeper" - And If You Fail, It Can Fine You and Send You to Jail for *Something Someone Else Did!*

Part 2 in a Series

when he receives the email on his Blackberry. VP Sales reads the Blackberry message while continuing with dinner and ordering two more glasses of Louis Treize cognac for his Chinese guest.

Those are the **background** facts. Fast forward **to the present**. Your company starts its *pre-acquisition due diligence* and, in the process, your staff discovers HinduMed's clever program to "convert a manufacturer's discount into an agent's commission." You - and your C-level acquisition counterpart from Stents - meet to discuss "this Indian mess" and to ponder: ***Whose problem is it?*** At the risk of telling you more than you really want to know, it's **everyone's** problem *if the acquisition goes through* - **except** perhaps the disgruntled employee who may in fact end up with a "whistleblower's reward." What you *care about most*, I'll bet, is whether **your company** is in trouble, and - come to mention it - whether **you're in trouble yourself**. And the answer is, if the acquisition goes through, **"Yes."**

Why Am I (and My Company, Of Course) in Trouble?

It's a "sins of the father" sort of thing. **Your company would be in trouble** because Stents, your acquisition target, would also be in trouble under *other laws* - the OECD Convention for Combating Bribery, for instance and the upcoming (next April) UK Bribery Act - and if your Company acquires Stents, *Stents'* troubles will become your troubles, because in most situations liabilities of the target **pass involuntarily** to the acquiror at closing.

As for yourself, **you'd be in trouble** because you knew (or during the course of the due diligence **would have had reason to know**) that violations of the FCPA by someone else you didn't even know had taken place thousands of miles away from your home office in the US. Whew! That's a pretty long story to illustrate ***vicarious liability***. But if you're really interested, you can click on the button just below to find seven recent real-life FCPA enforcement actions penalizing companies - and their executives - for acts done by or through agents and others. You will also see that the penalties are staggering and occasionally involve jail terms.

Fines and Jail Terms

Royal Dutch Shell (November 2010).

One of its subsidiaries hired a **customs broker** to make payments to Nigerian customs officials to obtain preferential treatment. Shell and the subsidiary have agreed to pay about $18 million in profits disgorgement and prejudgment interest to settle SEC charges.

Transocean, Inc. (November 2010).

Transocean made payments to an international **freight forwarder** and a **door-to-door courier service** to expedite the import of goods and equipment into Nigeria. Transocean has agreed to pay penalties of over $7 million to settle SEC charges. In related criminal proceedings, Transocean and an affiliate agreed to pay $13.4 million to settle DoJ charges.

Pride International, Inc. (November 2010).

Overseas subsidiaries of Pride made payments in multiple countries for illicit purposes, which payments (believe it or not) were not correctly recorded in the subsidiaries books and records, and consequently were incorrectly recorded on the books and records of the corporate parent. Pride has agreed to pay over $23 million in profits disgorgement and pre-judgment interest to settle SEC charges, together with related criminal penalties of over $32 million to settle DoJ charges.

Noble Corporation (November 2010).

Noble, headquartered in Switzerland but with an office in the U.S., authorized payments by its Nigerian subsidiary to the **subsidiary's customs agent** for forwarding to the Nigerian government in exchange for import permits. Noble has agreed to pay about $5.5 million in profits disgorgement and prejudgment interest, the amount of the penalties being reduced as a result of Noble's "self-reporting" and cooperation during the investigation. (More on the **pros and cons** of "self-reporting" next month.)

The U.S. Government Expects You to Be "Your Brother's Keeper" - And If You Fail, It Can Fine You and Send You to Jail for *Something Someone Else Did!*

Part 2 in a Series

Richard Bistrong (September 2010).

Bistrong, a former VP International Sales of Armor Holdings, a military equipment manufacturer, pleaded guilty to making $4.4 million in illicit payments to foreign government customers through **overseas agents** and **other intermediaries** and faces **five years** in prison and a $250,000 fine.

Juan Diaz (July 2010).

Diaz, a Florida business man, pleaded guilty to making about $1 million in bribes to Telecommunications D'Haiti, a government-owned telecoms company, on behalf of three U.S.-based telecoms companies. Diaz reportedly laundered the money **through another company**. He now faces **57 months in prison**, the forfeiture of over $1 million, restitution payments of $73,000 and **three years of supervised release after prison**.

John Warwick (June 2010).

Warwick, the President of Overman Assosciates, a U.S. engineering firm, as well as the former President of its **Panamanian affiliate** Ports Engineering Consultants Corporation (PECC), pleaded guilty to making about $200 million in illicit payments to former Panamanian government officials to secure no bid business concessions for PECC. Warwick now faces **37 months in prison**, the forfeiture of $331,000 and **two years of supervised release after prison**.

What Could I Have Done to Stay Out of Trouble?

Preventive measures, of course, are *fact-specific* and *"one size does **not** fit all,"* but here are some **due diligence** ideas you should consider instead of blindly exposing yourself and your company to vicarious liability for the actions of someone else.

- Inform yourself about your prospective business partner, sales agent, distributor, or consultant. Find out who its officers, directors and shareholders are and determine whether any of them (or their family members) are foreign government (or under the upcoming UK Bribery Act, foreign public) officials. Obtain and review its financial statements.
- Assess your prospective partner's credentials; determine whether it has and strictly enforces anti-corruption ethics and compliance policies.
- Conduct background checks through public or proprietary sources.
- Contact the U.S. Embassy or Consular Office in the countries or territories where your business partner will be representing you for "on the ground" information about its anti-corruption reputation.
- Interview your proposed business partner and ask about corruption issues in the countries or territories in which it will be representing you, how it has dealt with those issues in the past, and how it will deal with them as your business partner.
- Enter into a Foreign Business Partner Agreement detailing not only your prospective partner's ethical duties but also its compliance reporting obligations to you.

Coming Next.

Part 3 of this Series (next month) will focus what to do if you discover someone in your company may have committed an FCPA violation, whether that discovery is made by **your own people**, the U.S. or a **foreign government**, or a **whistleblower**.

The U.S. Government Wants to Put You in Jail for Breaking This Law . . . and Your Chances of Going Are Increasing!

Part 1 in a Series

John W. Brooks
Senior International Counsel
619.699.2410
jwbrooks@luce.com
www.luce.com/johnwbrooks

More Information.

For more information about the FCPA and how to create an effective FCPA Compliance Program for your company, please phone your principal Luce Forward lawyer or contact the author of this article at jwbrooks@luce.com.

SUMMARY

The Securities and Exchange Commission (SEC) and the Department of Justice (DoJ) are stepping up enforcement of the law known as the "Foreign Corrupt Practices Act." This comes in the face of continuing complaints by U.S. business leaders that the FCPA unfairly ties the hands of U.S. companies and their overseas affiliates by denying them the ability to compete on a level playing field with their direct competitors in other countries. But neither the SEC nor the DoJ is losing any sleep over these complaints. In fact, they're getting tougher.

Put 'Em in the Slammer. Less than a year ago the Attorney General in charge of FCPA enforcement at the DoJ said in a major policy speech that ***"Put simply, the prospect of significant prison sentences for individuals should make clear to every corporate executive, every board member, and every sales agent that we will seek to hold you personally accountable for FCPA violations."*** If his intention was to catch the attention of the U.S. business community, he clearly succeeded. Since then, the internet has buzzed with advice on what U.S. business leaders should do - not only how to comply with the law, but how to react if and when they're caught not complying with it.

Who's at Risk?

The FCPA covers ***all*** U.S. companies (big or little, public or private), together with all their employees and agents, all their overseas affiliates and partners, and ***all*** U.S. individuals wherever located.

What's the Law?

The FCPA prohibits bribery of foreign officials. There are ***five*** elements to an FCPA Violation: **1)** a payment or promise of ***anything of value***; **2)** to a foreign official, political party official, candidate for office or official of public international organization (Foreign Official); **3)** by you or your company, or its employees/agents in the U.S., or its employee/agents ***outside*** the U.S., or by a foreign person ***inside*** the U.S. assisting in the payment or promise; **4)** for the corrupt purpose of influencing an official act or decision of the Foreign Official; **5)** to assist you or your company ***obtain or retain business***, to ***direct business*** to any person, or to secure ***an improper advantage***.

Is That All?

No. You can be liable for a ***promise of payment***, even if payment is never made. ***Foreign officials*** include almost everybody even remotely connected to government, including officials of public international organizations, political parties and candidates for foreign political office - and perhaps even to their family members. ***Anything of value*** includes not only cash, but information, testimony of a witness, loans, promises of future employment, scholarships, sports equipment, trips, and the like. ***Corrupt intent*** means intending to induce the recipient to misuse his position or to influence someone else to do so. The business to be obtained/retained does not have to be with the foreign government, so long as the payment/promise is for the purpose of securing ***an improper advantage*** in obtaining/retaining any business with anybody. And finally, you don't have to know a payment by an overseas employee/agent will be passed on to a foreign official so long as you're aware there's a ***substantial possibility it might be***.

The U.S. Government Wants to Put You in Jail for Breaking This Law . . . and Your Chances of Going Are Increasing!

Part 1 in a Series

Who Enforces This Law?

The SEC enforces FCPA bribery and FCPA accounting violations by public companies, and the DoJ has exclusive jurisdiction over criminal violations. The SEC and DoJ share jurisdiction over civil violations.

What Are the Penalties?

The FCPA imposes both ***civil and criminal penalties***. Civil penalties for anti-bribery violations include fines up to $10,000 for companies or individuals ***per violation***. Civil penalties for accounting violations range up to $500,000 for companies and $100,000 for individuals ***per violation***.

Criminal penalties for anti-bribery violations include fines of up to $2 million for companies and $250,000 for individuals, again ***per violation***, and jail terms for individuals of up to five years. Criminal penalties for accounting violations range up to $25 million for companies and $5 million for individuals.

Note that these penalties are ***per violation***, and the FCPA cases brought by the government typically include ***multiple counts*** of alleged violations. In 2009, the average FCPA violation fine was $7 million and the highest was $579 million. Twenty individuals were indicted, and, as you might have guessed by now, an individual's fines are ***not indemnifiable*** by his or her employer or principal.

Recent Penalties Assessed

Just six years ago (2004), the DoJ brought only ***three*** FCPA criminal cases. In 2009, this number had climbed to **34**. This year the DoJ has over **120** open FCPA investigations. So far in 2010, the SEC and DoJ have announced civil and criminal fines against nine companies and 31 employees and agents amounting to **over $1.1 billion**, and the DoJ has obtained jail terms amounting to a **collective 16 years** for these employees and agents as guests in our federal prison system. Additionally, in the single largest FCPA prosecution ever against individuals, there are proceedings in progress involving over 20 company employees and agents with possible criminal fines in excess of $5 million and a collective 110 years in jail terms for the individuals involved.

A Glimmer of Leniency From the DoJ?

Effective just yesterday (November 1), the Sentencing Guidelines of the DoJ were amended to give compliance credit (lowering the penalty level) to companies like yours if 1) you have an ethics and compliance program (Program) in place with the persons responsible for the operation of the Program reporting directly to your Board or one of its committees, 2) your Program manages to detect an FCPA violation before it's discovered (or reasonably could have been discovered) by persons "outside" your company, 3) you promptly report the violation to the appropriate governmental authorities, and 4) no one responsible for the Program either participated in the reported violation, condoned it, or willfully ignored it.

Given the draconian consequences (only some of which are described above) of getting caught violating the FCPA, setting up a Program would seem to be a "no brainer."

Coming Next.

Part 2 of this Series (next month) will focus on the **types of FCPA risks** facing **you** and **your company** as a result of actions of **your overseas partners, agents and consultants** that you may know little or nothing about until you hear from your government - which, believe it or not - may want to put **you** in jail for **someone else's** actions.