FAIR MEASURES, INC.

P.O. Box 2146 Santa Cruz, CA 95063
831-458-0500, fax 458-0181
www.FairMeasures.com
training@FairMeasures.com

Managing Within the Law II

reference materials

We gratefully acknowledge the contributions to these materials of all of the attorneys who have worked with Fair Measures: Rita Risser, J. Logan, Jonathan Levy, Ann Kiernan, Steve Duggan, Lynne Eisaguirre, Julie Crane, Joelle Sullivan and Michele Huff. We also are grateful to our clients, and their legal counsel, Human Resource professionals and Training Department staff, who have given freely of their ideas to improve this course.

The Laws, Our Agreements and Ethics

The vast majority of people are ethical. They want to do the right thing and follow the law. They want to work for companies that are ethical, too. In the Ethics Resource Center's 2000 National Business Ethics Survey, 90% of the workers questioned said they expect their employers to do "what is right, not just what is profitable."

In addition to any standards of business conduct that employers may adopt, an array of laws govern every employee's actions. Some of these fall into the area of common sense or ethics, such as non-disclosure of proprietary information. Others may not be quite as intuitive, for example the laws governing insider trading and antitrust. All of these laws will be reviewed here.

The U. S. Federal Sentencing Guidelines require jail time for the violation of all of the laws covered in this section. And that's not all. There are also criminal penalties for violations of occupational safety and health laws, wage and hour regulations, and federal labor law.

When questions regarding correct conduct arise, it is the employee's responsibility to seek guidance. Under the law, every employee is required to report suspected wrongdoing immediately. This lessens the likelihood that the person reporting will be suspected as a participant in the illegal activity.

Employees who report, in good faith, misconduct by others are protected by law from retaliation. Reports may be made to management, Security, Human Resources, or the Legal Department.

Once a report is received, it is the responsibility of the company to investigate it. During the investigation, the company is required to take all steps necessary to maintain confidentiality. Of course there will be investigations where it is not feasible to be thorough and maintain confidentiality. In those cases names are released on a need-to-know basis.

If the company finds the law has been violated, it may be in its best interest to self-report the violation to the Government, as that reduces the possible penalties.

Violate These Laws, Go to Jail

These laws apply to all employees at the company. All of them have possible criminal penalties.

Protecting the Confidential Information of Others
Trade Secret Protection
Software Protection
Computer Misuse and "Hacking"
Financial Reporting
Reporting Information to the Government
Insider Trading
Export Control Laws
Political Activities and Contributions
Antitrust
Foreign Corrupt Practices Act
Doing Business with the Government
Kickbacks in Government Contracts

Sherron Watkins, a *Time* 2003 Person of the Year who "blew the whistle" on Enron's accounting practices, was fired by the company. Although firing whistleblowers is illegal in most states, the Texas Whistle-Blower Act applies only to government employees, so she was not able to sue. Congress passed the Corporate and Criminal Fraud Accountability Act of 2002, known as the Sarbanes-Oxley Act, in part to prevent that from happening to future whistleblowers.

The Act has many provisions, but we'll cover here those that relate to employees. The Act protects employees when they disclose information about fraudulent activities within their companies. In addition to filing a lawsuit under state law, the whistleblower employee may file a complaint with the Department of Labor within 90 days of the alleged retaliation.

Under the laws of most states, whistleblowers are entitled to emotional distress and punitive damages. Now under federal law, any person who "interferes with" the employment or livelihood of an employee for providing to a law enforcement officer any truthful information relating to the commission or possible commission of any federal offense, can be imprisoned for up to 10 years, and pay a fine up to $250,000.

This means that a manager can go to jail not only for firing a whistleblower, but also for demoting, refusing a promotion, or giving a negative reference.

The Act also requires companies, through their audit committees, to provide procedures for the confidential, anonymous complaints of employees' concerns about accounting or auditing matters. Employers may be able to use existing procedures for this purpose, if those procedures allow for confidential, anonymous reports.

The Act prohibits the destruction or alteration of documents, falsification of documents, or making any false entry in a document. This prohibition applies to any document relevant to the "investigation of any matter within the jurisdiction of any department or agency of the United States or any bankruptcy case, or in relation or contemplation of any such matter or case." The punishment is a fine and/or 20 years in jail.
Given the broad statutory language, this provision arguably applies to investigations by the Department of Labor into wage and hour violations, and by the EEOC into claims of discrimination and harassment, as well as workplace investigations of fraud and financial whistleblowing.

> **practical pointers:** Know your corporate ethics policy, and follow it. Be sure to manage and fire employees the right way to prevent claims of retaliation. Inform your employees on their responsibilities to prepare accurate documentation, and on the company's lawful document retention and destruction policy.

Agreements and Policies

Ethical leadership requires complying with any employment agreements and company policies, such as:

Disclosure of Confidential Information
Special Rules for Protecting Trade Secrets
Conflicts of Interest
Employee's Duty Not to Compete
Non-Compete Contracts With Former Employers
Interference with Contract
Gifts
Company Resources

Protecting the Confidential Information of Others

Employees should not solicit or accept from others confidential information about another company, under the mistaken belief that the information could benefit the company. The company has no interest in improperly receiving, and will not use, any proprietary or legally protected information of other companies.

If a manager hires an employee who has worked for another company doing similar work, naturally the manager wants the benefit of the employee's experience. But the employee cannot use proprietary information, even if the employee was solely responsible for developing the information. If in doubt, the manager should contact the Legal Department.

If an employee of a competitor offers confidential information, report it to the Legal Department.

Theft of trade secrets was made a federal criminal offense in 1996, in the Economic Espionage Act. Companies can be fined up to $10 million, and individuals can not only be fined up to $500,000, but also can be sentenced to serve up to 10 years in prison.

The Electronic Espionage Act was used in 2007 to prosecute a former Coca Cola employee who tried to steal company secrets and sell them to arch-rival Pepsi Cola. The former Coke employee was sentenced to eight years in prison, and her co-conspirators, who pleaded guilty and agreed to cooperate with prosecutors, got five and two-year jail terms.

In 2008, additional copyright enforcement powers were given to the Government in the PRO-IP (Prioritizing Resources and Organization for Intellectual Property) Act. This law allows a judge to order the impoundment of computers used to illegally download or reproduce copyrighted material, doubles the maximum fine for copyright infringement to $2 million, and allows for life imprisonment if someone dies or is grievously injured as a result of the trafficking of counterfeit goods or services.

Software Protection

The intellectual property laws (copyright, trademark) protect all software. It is illegal to copy software other than in compliance with the software's license. It is the policy of the employer to protect all software and other intellectual property from unauthorized or unlawful use, distribution and duplication. This policy applies to all software whether acquired by purchase or lease from outside vendors, received from

customers, or generated internally. All employees and departments are responsible for safeguarding software and technology in their possession from unauthorized use. Any unauthorized duplication of licensed software, except for backup purposes, is a violation of United States copyright law and of the copyright laws of other countries. Software may not be provided to outside third parties, including clients. Software may be used by employees at home for business purposes only after they consult with their supervisors to assure that the license for the particular software permits home use.

In 1997, President Clinton signed the No Electronic Theft (NET) Act. The NET Act provides for enhanced protection of copyrights and trademarks. Most notably, the NET Act permits federal prosecution of large-scale, willful copyright infringement even where the infringer does not act for a commercial purpose or for private financial gain.

The NET Act was used in 2006 in "Operation Fastlink," one of the largest multi-national law enforcement actions ever taken against online software piracy. Operation Fastlink has led to at least 35 criminal convictions in the US, as well as legal action in Belgium, Denmark, France, Germany, Hungary, Israel, the Netherlands, Singapore, Sweden, Great Britain and Spain. Nearly 100 individuals worldwide were identified by the investigation as leaders or high-level members of various international piracy organizations dedicated to the illegal reproduction and distribution of copyright protected software, including movies, games, music and business utility programs.

Computer Misuse, Including “Hacking”

Enacted in 1984, long before the Internet revolution, the federal Computer Fraud and Abuse Act made it a crime to “hack” into government and bank computer systems. That statute has been modernized and expanded to cover all computers used in interstate communications. It is a federal offense to obtain unauthorized access to a computer and obtain information from it. It is also a crime to get unauthorized access to a computer and commit fraud or other dishonest wrongdoing. The severity of the punishment depends on how much harm was caused.

In addition to its use in criminal prosecutions, this Act can also be used by private companies to recover damages to compensate them for the harm done by unlawful computer use. Companies have used it to go after spammers, hackers, frauds, and trade secret thieves. In a 2006 federal appeals case, an employee used a secure-erase program to wipe

data off his company laptop before the turned it in and quit to start a competing business. His ex-employer sued under CFAA and won, the court finding that he was no longer an authorized user of the system once he had decide to destroy the files that showed he had breached his duty of loyalty to his employer.

The Digital Millennium Copyright Act (DMCA) was signed by President Clinton in 1998. The legislation implements two 1996 World Intellectual Property Organization treaties and addresses a number of other significant copyright-related issues. It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures (commonly known as digital rights management or DRM) that control access to copyrighted works and it also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself. In addition, the DMCA heightens the penalties for copyright infringement on the Internet, while limiting the liability of internet service providers for copyright infringement by their users.

In 2007, a California man who had fraudulently activated more than 179 subscriptions of Microsoft Developer Network Software pleaded guilty to DCMA charges and was sentenced to serve 20 months in federal prison and to make restitution of $500,000—the value of the stolen software subscriptions—to Microsoft.

Financial Reporting

Public companies report a great deal of financial information both to the public and to the Securities and Exchange Commission of the United States government ("SEC") so that investors can make decisions whether to buy or sell company stock based on accurate data. As a result, companies are subject to various securities laws and regulations. If inaccurate or misleading financial information is disclosed, a company's status as a public company would be directly affected.

Because a company's financial disclosures are often based on information compiled from its various divisions, all employees must participate in the process of ensuring that the information disclosed by the company is complete and truthful without omission, concealment, or falsification of information. False information from an employee about a single transaction can affect the financial disclosures a company makes to the public and to the SEC. For example, a significant component of a company's financial reporting is the disclosure of its sales revenue by quarter. If a particular sale is recorded in the wrong quarter--based on

inaccurate invoices or shipping records or other internal documentation--the error can result in inaccurate information in the company's financial disclosure.

Accuracy and completeness in the recording and reporting of information, an activity in which virtually every employee is involved, is a critical commitment.

- Don't make false or misleading statements to other companies with which we do business about contract specifications, pricing, product source, financing, etc. This applies to customers, suppliers, distributors, banks, and all others in the business community.

- Don't make false or misleading entries in any company record.

- Employees are responsible for verifying all information they provide.

- Information must never be presented in a way that is designed to mislead, such as intentionally omitting important data or purposely leaving spaces on a form blank to avoid reporting the truth.

- Employees must not sign or certify documents they have not actually read and verified.

- Employees must retain records for the periods of time specified in company policy and safeguard such documents from loss or destruction.

- Never act on someone else's "hot tip" that might be based on inside information, That's just as illegal as trading on inside information about your own company.

- Don't give out untrue or misleading information that others might think is an insider tip.

Dishonest, incomplete or inaccurate reporting is contrary to company policy. It may also subject an employee to civil or criminal penalties for false statements or for fraud.

Reporting Information to the Government

Many times, company employees are called upon to make reports to government authorities in the U. S. and various countries in which the company does business. For example, employees may need to fill out customs or other forms, answer questions by government inspectors or

respond to government inquiries. It is critical that all such reports to governmental agencies be accurate and that they not omit any material information. If a government agent has filled out a portion of a form incorrectly, the employee should not sign it or otherwise agree to it without correcting the error. Even if a particular question seems to be an insignificant one, employees must respond fully and accurately. Any misrepresentation or omission to a government authority violates the law. It can subject the employee and the company to civil and criminal penalties.

If you have any questions about a particular entry or report to a government authority, consult with your supervisor or the Legal Department.

Insider Trading

In the course of your employment, you may become aware of significant information about the company or other companies that has not been made public. There are strict requirements regarding the disclosure of such information. The general rule can be stated as follows: Material inside information must not be disclosed to anyone, except to persons within the company whose positions require them to know it, until it has been publicly released by the company.

Examples of material inside information include:

- financial information
- company plans to make acquisitions
- earnings changes
- extraordinary sales or expenses
- anticipated successes or difficulties
- new contracts or products
- major organizational changes

It is a violation of U.S. federal securities laws for any person to buy or sell securities if he or she is in possession of material inside information. Information is considered material if a reasonable investor would consider it important in arriving at a decision to buy, sell, or hold shares of the company's stock. Until material information is released to the public, it is referred to as "inside information" because it may be known only to insiders of the company such as its officers, employees, agents or others who have access to confidential information.

It is also illegal for any employee in possession of material inside information to reveal that information to anyone else. Both the insider who provides the confidential information and the person who trades in stock based on the information can be held liable for insider trading. It is illegal to disclose the information even if you have no knowledge of the intent of the other person to trade illegally. There is no such thing as an "innocent" disclosure.

In fact, one of the largest insider trading cases in history started when an IBM secretary gave her husband a tip on an upcoming deal, which she had first learned about while making photocopies.

The case began when the secretary, Lorriane Cassano, told her husband Robert that IBM's board had authorized making an offer to acquire Lotus. He told two friends, including one man whose brother owned a delicatessen. The delicatessen owner then allegedly told some of his best customers, including a doctor who stopped by for lunch. Others, including a pizzeria owner, bank vice president, teacher, grocery store owner, lawyer, president of a direct-mail marketing company, two computer technicians, and several stockbrokers, quickly learned by word of mouth.

Within hours that day, nearly 20 people had bought stock, betting that IBM was about to acquire Lotus Development Corp. When the deal was announced three days later, the group made a whopping $1.3 million profit, although the secretary and her husband gained only $7,500.

But those gains were short-lived. The Securities and Exchange Commission investigated and brought criminal charges. Ms. Cassano was suspended, then fired for violating IBM's strict policy against disclosure of non-public information. Her husband pleaded guilty to insider trading, and was sentenced to probation after agreeing to cooperate with investigators. The Cassanos also had to repay their profits. Other participants in the scheme (who made things worse by trying to conceal their activities, lying under oath to investigators and falsely denying they knew each other), pleaded guilty to charges including conspiracy, obstruction of justice, insider trading and perjury, and had to repay their ill-gotten gains, as well.

To avoid the prohibitions on insider trading, all employees must follow certain steps:

- No employee may disclose material inside information for any reason to anyone--even family members--until the information has been publicly disclosed by the company.

• Employees should not buy or sell the company's stock based on material inside information until the third working day after the information has been announced to the public.

• No employee may buy or sell the stock of another company that may be affected by actions of the company which have not yet been publicly disclosed.

• Employees must observe the no trading periods set forth in the Insider Trading Policy.

U. S. Export Control Laws

The purpose of the U.S. Export laws is to control the transfer of certain items, technologies, and services to certain countries, in order to promote U.S. national security, foreign policy, nonproliferation, and short supply interests.

The law is driven by (1) the country to which the export is intended and (2) the type of product being exported.

Some countries are embargoed by the U.S., and no products can be sent there. As of January, 2009, the embargoed countries are: Cuba, Iran, North Korea, Sudan, and Syria. (There are some exceptions for humanitarian aid, and additional exceptions for Syria.)

Depending upon the type of item, technology or service being exported, there are also other prohibited export destinations. What are considered export controlled items and technology? Examples include high performance computers and related design information, encryption, and microprocessor development information.

NOTE: It may be legal to export a high performance computer, but not legal to export the development source code.

An export is more than sending a physical object to another country. "Exports" include not only sales of hardware or software, but also the transfer of information by:
--talking on the phone, in meetings or in tele-conferences
--carrying a laptop computer loaded with export controlled information
--sending an e-mail or fax
--hosting visitors from foreign countries

--sharing information with employees, subcontractors, vendors, joint venturers, customers, subsidiaries, affiliates.

Managers who supervise employees who work with high technology information should be aware that an export license from the U.S. government must be obtained before giving access to a person who is a foreign national of an embargoed or controlled country (whether the person is living in the U.S. or elsewhere). Transfer of controlled information to a foreign national is considered to be the same as an export to the person's home country.

If you work with high technology, you need to be aware of your duties under the law.

In hiring, the hiring packet that you receive from Human Resources upon approval of the requisition includes applications for employment, and with those applications are notices to the applicants of export control requirements. It is your responsibility to get those applications and notices to all candidates at the beginning of the interview process. Offers of employment may be contingent upon receipt of export licenses from the government.

If you are considering retaining a consultant or contractor, or hosting a visitor who will be exposed to high technology information, notify the appropriate department to find out if they may need export licenses.

All employees traveling to a controlled country with high technology products (including samples), documents, or data (including data contained in a computer system) must receive clearance before traveling.

The U. S. government can impose civil and criminal penalties against an individual and the company for violating the U. S. export control laws. The penalties against the individual are up to $250,000 per violation, and up to 10 years in prison. Penalties against companies are up to $1 million per violation or five times the value of the export, whichever is greater, and the company may no longer be allowed to export.

Political Activities and Contributions

Companies are prohibited from contributing directly to candidates for office in the federal government of the United States.

Companies may establish Political Action Committees under applicable laws to support the election of candidates for federal, state and local office. Political Action Committees are supported by voluntary contributions of employees using their own personal funds.

Employees are encouraged to individually participate in the governmental and political process, but it must be understood that the employee will bear the entire financial responsibility for such a contribution. Additionally, if an employee wishes to speak out on political issues, the employee must do so as an individual and not speak as a representative of the company. If you have any questions about a particular political activity, campaign or contribution, you should consult the Legal Department.

Antitrust: Protecting Competition

The antitrust laws are designed to protect competitors against unfair business practices and to promote and preserve competition. They prohibit different types of agreements among companies to restrain free trade, efforts by companies to monopolize the marketplace, to fix and control prices, to boycott certain customers or suppliers, and other types of anti-competitive conduct.

Companies can compete vigorously and ethically, but still support free trade throughout the world and comply with the antitrust laws. All employees (particularly those involved in sales and marketing) should become generally aware of the fundamental principles of antitrust laws. The following guidelines, while not intended to be all-inclusive, are designed to present some examples of actions challenged under the antitrust laws.

Monopolies

Monopolies (from the Greek: *mono*= one and *poles*=seller) are not illegal. But, using unfair tactics to become or maintain a monopoly violates the antirust laws. So does using your dominant market position—which can be as little as 50% of the product or geographic market--to control prices or exclude competitors.

That's what the federal appellate court found in the *U.S. v. Microsoft* antitrust case in 2001. Microsoft, which had a 95% share of the market for Intel-compatible PC operating systems, was clearly a monopolist. The appeals panel found that Microsoft had improperly used its monopoly power by:

- preventing computer manufacturers from pre-installing Netscape, in addition to Internet Explorer (IE);
- entering into exclusive contracts with 14 of the top 15 internet access providers, which insured that subscribers were offered IE either as the default browser or only browser;
- forcing Apple Computer to offer IE as the default browser, as a condition of Microsoft's agreement to continue supporting and updating the Mac Office software suite;
- coercing Intel to stop aiding Sun Microsystems in improving its Java technologies;
- deceiving Java developers into writing applications that would run only on Windows;
- requiring software developers to use Microsoft's version of Java instead of Sun's.

Other examples of improper use of monopoly power in other cases include selling a product below cost, also called predatory pricing; making untrue statements about a competitor's product; hiring away a competitor's key employees, with the intent of crippling the competitor; raising competitors' costs in order to disadvantage them; and using monopoly power in one product to force purchasers to buy another one, also called an illegal tie-in.

Contact with Competitors

The antitrust laws specifically prohibit agreements or understandings, expressed or implied, between competitors concerning prices, territories, customers or other aspects of the competitive marketplace.

From 2001-2008, the U.S. Department of Justice garnered an unprecedented $3.5 billion in criminal price-fixing fines against 120 corporations and 160 individuals. Included in that sum is a $300 million fine against Samsung Electronics in the dynamic random access memory (DRAM) chip case, and $134 million against Mitsubishi Corp. in price-fixing of graphite electrodes. The results came from an amnesty program that gave a pass to the first company to confess involvement in a cartel and identify other participants. The punishment got worse for those that followed in the door with confessions, but allowed breaks for those that identified price-fixing in previously uninvestigated industries.

To prevent antitrust violations, experts recommend:

• Do not meet or talk with competitors for any reason unless discussing a purchase from or sale to the competitor or during a trade association activity that has been approved by the company. Any other conversation should be cleared in advance with in-house legal counsel.

• Do not exchange or discuss any competitive information including prices, costs, purchases or sales.

• Do not give the company's price list to a competitor and never accept a price list from a competitor.

• Do not engage in shop talk or war stories with competitors about particular customers or other competitors.

• If you are contacted by a competitor who attempts to discuss competitively sensitive information such as prices, costs or customers, you should immediately report the contact to the Legal Department.

• You should immediately leave any meeting, even an approved trade association meeting, if anyone attempts to exchange or discuss competitively sensitive information, and announce why you are leaving.

• You should refrain from criticizing a competitor's product and focus on marketing the positive attributes of the company's products.

Customers and Suppliers

Companies are free to determine how and with whom they choose to do business.

• Customers are free to determine the prices at which they resell a company's products. Another company may not dictate the prices at which customers resell the company's products.

• It is permissible to send a distributor a printed price list that suggests resale prices.

• If a distributor/customer is also a competitor, all discussions, particularly price discussions, should be limited to the particular products being sold to that customer.

Experts recommend as general guidelines:

• Do not require customers to pass along any price reduction.

- Do not discriminate, in price or otherwise, among customers. Price should not be used as a method to discipline distributors.

- Do not require a customer to purchase one item in order to be able to purchase another product or service from the company.

- Do not require the purchase of the full line of the company's products.

- Do not prohibit a purchaser from dealing in a competitor's products.

- Do not require or agree to exclusive buying or selling arrangements.

In general, employees should never enter into any agreements or understandings with employees of other companies on the topics outlined without consulting the Legal Department. Even if such an agreement does seem reasonable to the employee for some proper business purpose, it should be discussed with management. And, finally, all contracts and arrangements between two companies should be reviewed and approved in advance as per policy.

Foreign Corrupt Practices Act

All employees who have any management, accounting, operational, or sales responsibilities for activities outside of the United States must be aware of the Foreign Corrupt Practices Act and its impact upon operations.

The Foreign Corrupt Practices Act ("FCPA") was enacted in the United States to specifically prohibit payments by United States' companies and their subsidiaries to government officials in foreign countries in order to secure business or otherwise influence the judgment of the official. This prohibition also applies to payments or offers of anything of value to intermediaries, sales representatives, or agents if the employee knows, or has reason to know, that the payment or offer will be used for a prohibited payment, gift or favor. Additionally, the FCPA requires companies to establish a system of internal accounting controls and to maintain accurate and reasonably detailed books and records.

As a result of SEC investigations in the mid-1970's, more than 400 U.S. companies admitted making more than $300 million in questionable or illegal payments to foreign government officials, politicians, and political parties. The abuses ran the gamut from bribery of high foreign officials to secure some type of favorable action by a foreign government to so-

called “facilitating” payments made to ensure that government functionaries discharged certain ministerial or clerical duties. Some of the abuses led to serious foreign policy problems for the United States, since the revelation of improper payments embarrasses friendly governments, lowers the esteem for the United States around the world, and lends credence to allegations that American companies exert a corrupting influence on the political processes of other nations. Congress enacted the FCPA to bring a halt to the bribery of foreign officials and to restore public confidence in the integrity of American business.

The FCPA prohibits payments by:

- Employees are to conduct business in compliance with the laws of all countries in which the company does business.

- The use of company funds for any unlawful or improper purpose is prohibited.

- Any use of company funds shall be disclosed and recorded.

- No accounting record shall be falsified, inflated, or disguised in any manner.

Although highly discouraged, it is not a violation of the FCPA to make minor, insubstantial payments, gifts, favors or other benefits (i.e., facilitating payments) to low-ranking foreign government officials whose duties are essentially ministerial or clerical, and where no reasonable alternative exists, to obtain the prompt performance by them on routine governmental action, such as the issuance of customs clearances and residency permits. (No payment, however, should be made to cause such officials not to perform their duties.)

Whether such payment is prohibited depends on the circumstances, and employees should make sure that any such payment has been officially approved by an authorized individual within the company. In every case, all such minor payments or gifts should be clearly and accurately recorded in the company's books and records. If there is some reason why a payment should not be recorded, then there is some reason to believe that the payment is improper, and it should not be made. No unrecorded or off-the-record accounts are to be maintained for any reason. Similarly, there is no reason why any legitimate payment must be made in cash or to an unidentified account.

If there is any doubt as to whether the payment, gift, favor or other benefit is permitted under these rules, you should consult with the Legal Department.

While the FCPA was the first anti-bribery statute of its kind in the world, it was largely symbolic for its first twenty years, since the Government brought a total of only 33 enforcement actions during that time. However, since the late 1990's there has been much more vigorous enforcement of the law. In 2008 alone there were 33 enforcement actions, the same number as in the FCPA's first two decades. The potential penalties are severe, indeed. Corporations and other business entities are subject to criminal fines of up to $2,000,000; officers, directors, stockholders, employees, and agents are subject to a fine of up to $100,000 and imprisonment for up to five years. Moreover, under the Alternative Fines Act, these fines may end up even higher -- the actual fine may be up to twice the benefit that the defendant sought to obtain by making the corrupt payment. And, fines imposed on individuals cannot be paid by their employer.

In addition to criminal prosecution, the Government can also bring a civil action for a fine of up to $10,000 against any firm as well as any officer, director, employee, or agent of a firm, or stockholder acting on behalf of the firm, who violates the antibribery provisions. In addition, in an SEC enforcement action, the court may impose an additional fine not to exceed the greater of (i) the gross amount of the pecuniary gain to the defendant as a result of the violation, or (ii) $100,000 for a natural person and $500,000 for a business.

Under guidelines issued by the Office of Management and Budget, a person or firm found in violation of the FCPA may be barred from doing business with the Federal government. Indictment alone can lead to suspension of the right to do business with the government. In addition, a person or firm found guilty of violating the FCPA may be ruled ineligible to receive export licenses; the SEC may suspend or bar persons from the securities business and impose civil penalties on persons in the securities business for violations of the FCPA; the Commodity Futures Trading Commission and the Overseas Private Investment Corporation both provide for possible suspension or debarment from agency programs for violation of the FCPA; and a payment made to a foreign government official that is unlawful under the FCPA cannot be deducted under the tax laws as a business expense.

2008 was a record enforcement year for the FCPA. In December, 2008, Siemans AG and several of its subsidiaries pleaded guilty to some FCPA

criminal charges and agreed to settle an SEC enforcement action. Under the plea agreement and civil settlement, Siemens and its subsidiaries agreed to pay a total criminal fine of $450 million and to disgorge $350 million in illicit profits to the SEC, the largest monetary sanction ever imposed in an FCPA case since the act was passed by Congress in 1977. Siemens also consented to an SEC injunction against future violations of the FCPA and agreed to retain an FCPA compliance monitor for up to four years.

Doing Business with the Government

When companies enter into contracts to provide goods, services and technology to government entities, including the United States federal government, special care must be paid because activities that might be appropriate when dealing with private sector customers may be improper and even illegal when dealing with the Government. In dealing with the Government, companies must be forthright and candid. Any information supplied to Government officials must be accurate and complete.

It is critical that no employee ever misstate or omit material information in dealing with the Government as it may violate the law and give rise to serious sanctions. This prohibition extends to all information, whether oral or in such written documents as proposals, bids, or invoices. It also applies to any representations about the company (such as the number of its employees or the identity of its subsidiaries) or about the source of the goods it provides. It also refers to pricing data, since Government contractors are routinely required to provide such information to demonstrate how they calculated their proposal. Misrepresenting pricing data in such circumstances is strictly prohibited.

Employees must never make any misrepresentations to the Government about the type or quality of products or services that the company is providing. For example, it is strictly prohibited to provide the Government with a product that does not meet Government specifications without disclosing the variance, since doing so may amount to a representation that the product meets Government specifications.

The Government must be billed only for costs that are properly chargeable to the contract. Extreme care must be taken in allocating costs such as subcontractor charges and material costs so that the Government is not charged for something not properly attributable to its contract.

The Government must be billed according to the actual hours worked by employees. Employees working under Government contracts must exercise extreme caution to ensure that their time cards are accurate and that the number of hours they claim to have worked is correct. Inflating the number of hours or of employees chargeable to the Government is strictly prohibited. Time spent working on one Government contract may not be charged against another Government contract.

Certain steps must be taken by employees to ensure the integrity of the Government procurement process. No employee shall offer, give or promise to give any federal employee or representative any item of value, including transportation, entertainment and/or meals, unless the item has no or minimal monetary value. During the course of a federal procurement, no employee shall offer or discuss the possibility of future employment with any federal employee or representative (including contractors, consultants, and experts) who has participated personally and substantially in the procurement. Violation of this rule led in late 2003 to the firing of Boeing's Chief Financial Officer, who had discussed the hiring of a senior Air Force procurement official with her while she was still considering Boeing contracts, and the resignation of Boeing's CEO a week later.

Finally, employees must not take any steps to solicit or obtain "proprietary" or "source selection" information concerning a procurement. This includes information that the Government uses internally to determine to whom a contract should be awarded and is generally not disclosed by the Government. Such information might consist of bids or price proposals, competitive range determinations, rankings of offerors, technical, cost or price evaluations, and source selection information. These items are based on information submitted confidentially to the Government by competitors or developed by the Government confidentially, and efforts by a company to obtain the information are strictly prohibited.

Kickbacks

United States federal laws prohibit the offering, soliciting, or accepting of any kickback as well as including the amount of any kickback in a contract with the United States. A kickback is considered to be money, credit, gift, gratuity, anything of value, or compensation of any kind which is provided for the purpose of improperly obtaining or rewarding favorable treatment in connection with a contract in the United States. If an employee has any reason to believe that a violation of kickback laws has occurred, the employee should immediately contact the Legal Department.

Disclosure of Confidential Information

The Employee Agreement every employee signs generally provides that the person will, at all times during and after employment hold in strictest confidence any trade secrets or confidential or proprietary knowledge or information concerning any inventions, mask works, manufacturing or processing techniques, processes, formulae, data, including software products, or other matter relating to the research and development programs, products, customers, sales or business of the Company.

Generally, there are three types of data that are covered: company confidential (non-proprietary), company proprietary confidential, and company restricted - trade secret. Company confidential (non-proprietary) information can be shared with anyone in the company. Company confidential proprietary information can be shared only with employees who need to know. Company restricted - trade secrets are subject to strict access controls.

Employees must protect all of this information. This applies not only to company information, but also to proprietary and private data entrusted to the company by customers, joint development partners, suppliers, or other business partners. Wholly apart from the concerns about insider trading outlined earlier, disclosure of confidential, proprietary or trade secret information--even if it is inadvertent--can harm the company's interests and violate the trust that has been placed in you by the company and by your fellow employees.

For example, you must not discuss with others the company's earnings or other financial information that has not been made public, confidential marketing or service strategies, or secret business plans, as this information is of competitive value to the company. Furthermore, you should exercise care in discussing confidential information even with fellow employees when others might overhear your conversations--for instance, at a trade show, at a restaurant or in an airplane.

As difficult as it is, you should not discuss confidential information with family members, close friends or therapists. By making it a rule never to discuss confidential company matters with those outside the company, you avoid placing both yourself and them in difficult situations. And you should remember that even the smallest and seemingly most harmless disclosures can add up--bits of information can be pieced together to provide a much fuller picture than you intended to convey.

If approached for information by someone outside the company, employees should not attempt to answer questions. If you have a question about how a particular inquiry should be directed, consult with your supervisor or the Legal Department.

Conflicts of Interest

Conflicts of interest can arise when an employee's personal interests conflict with those of the company. While employees are free to lead their lives outside the company as they see fit, they should avoid situations that create or appear to create conflicts of interest or divided loyalty. Such circumstances are not automatically prohibited, and should not be entered into without prior written approval by the company.

It is difficult to catalog the various ways in which a conflict of interest can arise. Here are some examples:

- Employees should not engage in employment or other activity which interferes with their work. This relates both to time requirements of employment and their duty not to put themselves in a position that might create a conflict of interest with the company.

- Employees should not be employed by or provide any services to a company which does or seeks to do business with the company as a supplier, or with a competitor of the company.

- Employees should not borrow money from, or enter into any personal financial transaction with, a company that does or that is seeking to do business with the company, other than arms-length transactions with recognized commercial banks or financial institutions.

- Employees should not perform outside work or solicit for outside work on company premises or on company time.

In determining whether a conflict exists, an employee should include in these prohibitions family or other personal relationships (such as a spouse or child, or another relative the employee supports or is otherwise involved with financially). For example, just as an employee may not borrow money from a company supplier, the employee's family members should not borrow if such action would create the appearance of a conflict of interest.

Because it may be difficult to determine whether particular circumstances give rise to a conflict of interest, employees should discuss these issues with management or the Legal Department. If an employee feels uncomfortable reporting the circumstances, that fact strongly suggests a conflict does exist and the situation should be avoided.

Gifts

Employees should not accept gifts, entertainment, or gratuities from suppliers, competitors, customers, vendors, or any other entity that the company does business with unless (1) the gift is of nominal value and, (2) the gift cannot be construed as a bribe, payoff, or improper inducement.

Employees should never accept gifts in cash or cash equivalents.

Company Resources

Protection of company assets is important as all of the company's resources are vital to its success as a business. For this reason, all employees should be individually responsible for protecting company assets.

- Misuse, misappropriation, or theft of company property is absolutely prohibited. This includes any company funds or company assets, such as software, telephones, computers, copy machines, facsimile machines, supplies, and any other property owned by the company.

- Use of company property, such as computers, copy machines, and telephones must be limited to company-related work. Occasional, reasonable personal use is allowable. Reasonable use depends upon the circumstances and is subject to review by management.

- E-Mail. The company's e-mail system should be used by employees for business purposes. Occasional, reasonable personal use is allowable. Reasonable use depends upon the circumstances and is subject to review by management.

- Under federal telecommunications laws, the contents of all data files on the company's system are the exclusive property of the company. E-mail messages are the exclusive property of the company, and the company reserves the right to monitor and review any and all e-mail messages, without notification to employees. Employees should not expect that any message put into the e-mail system is a private communication. Furthermore, any use of the e-mail system to exchange

messages of a derogatory, discriminatory, harassing, or otherwise improper nature is absolutely prohibited.

General Legal Duties

If someone threatens to sue, you should say in a calm manner, "I believe I'm right. I'll be glad to consider an outside opinion if you want to get one. Until then, I expect you to follow my instructions."

If an employee does present you with an opinion letter from an attorney, check with your attorney to make sure your decision was right.

When you consult a lawyer—either in-house counsel or an outside firm--about a legal issue, your discussions are covered by the attorney-client privilege. That means neither you nor the lawyer can be compelled to reveal your questions or the advice you were given.

The purpose of the attorney-client privilege is to allow you and your lawyer to consult confidentially. Tell your lawyer the truth, the whole truth, and nothing but the truth. Even if you are embarrassed and realize you fouled up, tell your lawyer exactly what happened, so you can get the best advice possible under the circumstances.

The attorney-client privilege belongs to the client: your company. But you can forfeit the whole company's attorney-client privilege by revealing your conversation with the lawyer to any outsider. To preserve the privilege, do not talk to ANYONE about company legal matters unless the Legal Department or your outside attorney has authorized it. This includes your spouse or life partner, other family members, friends, and former co-workers.

If a government or private investigator arrives at the premises you supervise and asks for information or to make an inspection, ask to see the investigator's identification, and call your Legal department or outside counsel for further advice.

Contact your attorney IMMEDIATELY if you get any notification of legal action, such as: a letter or telephone call from an employee's lawyer; a letter threatening a lawsuit; a subpoena to testify and/or produce documents; a search warrant; a summons and complaint; or notice of inspection by a government agency. Do not attempt to handle these legal proceedings by yourself!

During litigation, the parties to the suit are supposed to preserve all the evidence until the case is over. Do not try to "outsmart" the court, the Legal Department or the other side to the case by hiding, altering, or

destroying relevant documents or other evidence. If you get instructions from Legal to keep all files on a certain subject, make sure you follow those instructions. In Zubulake v. UBS Warburg, a 2005 federal gender discrimination case, UBS's counsel — both in-house and outside — instructed UBS personnel to save relevant electronic information. Notwithstanding these instructions, certain UBS employees deleted relevant emails. Other employees never provided relevant information to counsel or provided it years after the request had been made. As a result, the trial judge told the jury that UBS had willfully destroyed the emails and that the jury could conclude that the missing emails would have supported the employee's claims of discrimination and retaliation. The jury returned a $29 million verdict in the employee's favor.