Corporate Compliance Programs: Weaving an Effective Compliance Web

Simply put, corporate compliance programs are designed to prevent and detect violations of the law. Compliance programs make good business sense because they: reduce the likelihood of a violation of the law; lower the costs of a violation; and build a values-based culture. In spite of these benefits, compliance programs are not as prevalent as one would imagine.

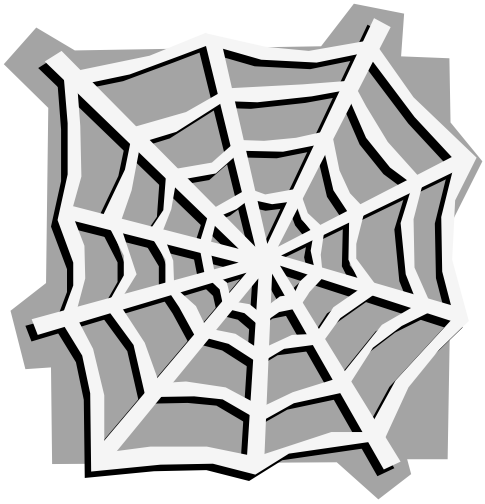
In many ways, an effective compliance program can be compared to an intricate spider web – they need to be designed to detect and catch violations from a variety of different angles. They must also be tailored to the unique needs of each organization – not one size fits all. Lastly they need to be resilient – strong but flexible.

This paper explores some of the key drivers behind an effective compliance program. Ultimately, each company must determine what works best for its unique set of issues; however, the following considerations are likely to be relevant to a wide range of organizations.

THE SPIDER AND THE FLY: WHO SHOULD CARE?

Today's corporate climate has been greatly influenced by widely publicized events of corporate fraud and scandal. Enron, Arthur Andersen, Worldcom, Adelphia, Imclone, Tyco – and the list goes on. Not only have these organizations been involved in criminal and civil legal proceedings, but in many instances, their most senior officers and directors have been implicated. In response to these scandals, the Sarbanes-Oxley Act of 2002 (***SOX***) was enacted and represents the federal government's furthest reach into corporate governance.

While a majority of the provisions of SOX apply to public companies, private companies are affected as well. There is a growing recognition that private companies will be well-served to adopt best practices mandated under SOX. Good corporate governance is becoming a significant factor in a range of relationships including those with lenders, insurers, investors and potential M&A partners. Companies that do not adhere to SOX-level governance and compliance will be disadvantaged in those relationships. For example, a private company that is unable to demonstrate adequate internal controls may be eliminated as a potential acquisition candidate by a public purchaser over fear of unreliability of reported financial results. Moreover, in any lawsuit alleging financial mismanagement, fraud, corporate waste, oppression of minority shareholders and similar actions, a plaintiff will surely seek to measure the adequacy of corporate governance and internal controls against the SOX yardstick. Finally, SOX expanded the scope of various federal offenses relating to obstruction of justice and retaliation against "whistleblowers" – people that point out or raise concerns about possible illegal activity. These penalties emphasize the importance, even for private companies, of adopting effective compliance programs that contain policies regarding document management and retention and protection of whistleblowers. In any event, whether private or public, SOX should be seen as a catalyst for broader review of a company's governance and compliance programs.



SPINNING THE WEB

Good compliance programs begin and end with the company's Board of Directors. The directors have ultimate responsibility for setting up a comprehensive program and making sure that it works over time. Three main areas must be addressed at this level are: adopting a comprehensive compliance program; delegating authority to key management for the direct implementation; and oversight of the program.

An established line of court cases, including the seminal *Caremark* decision in Delaware, makes clear that directors have an affirmative duty to assure that their companies have an adequate information and reporting systems in place. This duty is clearly underscored by SOX. However, having policies in place but not following them may be worse than having no policy at all – witness Enron. Therefore directors' duties are not discharged simply by adopting a program and putting it on a shelf. Effective delegation and oversight are critical.

The next level of implementation rests with the Chief Executive Officer who is responsible for setting a tone of compliance. Success requires shared vision of the goals. The CEO typically is the person most responsible in the organization for communicating this vision to the employees. The CEO must make clear that employees who do not follow the rules, will be held accountable for their failure to do so. Currently, there is great pressure on companies to achieve more with less. In this environment, compromises on compliance issues must be resisted. The message must be clear: making numbers is important but making them in an acceptable manner is paramount.

In a tight economy, many companies are loath to allocate additional budget to areas that do not have a direct link to improving the bottom line. However, in an era of reductions in force, the likelihood of a disgruntled employee reporting a violation, real or perceived, is greatly increased. In addition, prosecutors that had few white-collar fraud cases on their dockets in years past have new ammunition under SOX and a spotlight in which to pursue these claims. In this environment, it is easier and less costly to build a reliable compliance program at a reasonable pace than it is to respond to a charge by law enforcement or regulatory officials. Even if charges are brought, companies and their officers and directors are entitled to reduced penalties and greater protections against certain types of liabilities by virtue of having well-designed compliance policies in place. Smart companies will understand that this means increased time and resources must be devoted toward implementing and upgrading effective compliance programs.

The final component to establishing a compliance program is providing for the day-to-day administration of the program. This will vary widely depending on the size and complexity of the organization. Many companies can effectively utilize a single compliance officer. In larger organizations, a committee of business unit leaders may be more appropriate. Regardless, the role of the compliance officer must be clearly communicated and clear policies, standards of conduct and procedures must be established. The program must answer the following basic questions: who does what, when, how and for whom. Lastly, remember – compliance programs are not a one shot deal; they require reliable and recurring training, monitoring and enforcement.

THREADS OF THE WEB: WHAT COULD GO WRONG?

Compliance programs need to be reasonably designed to establish standards and procedures that are capable of detecting and reducing violations of law. Just as each spider web is unique, the actual criteria for any given compliance program – the threads of the compliance web - will be different for each entity. As a result, the first step in developing an effective compliance program is risk

assessment. This process is akin to undertaking due diligence on an entity that might be a potential acquisition candidate. Ask the following questions:

- What are the key regulatory drivers that affect the business?
- What areas do we know where we have imperfect compliance?
- What are the areas in which non-compliance is most likely to occur and why?

In the risk assessment stage, companies must take a comprehensive look at their business and they are well-advised to consult with outside counsel to understand and consider the legal framework applicable to the business. For example, companies with international operations need to be aware of the antibribery provisions of the Foreign Corrupt Practices Act that make it unlawful for a U.S. person to make corrupt payments to foreign officials for the purpose of obtaining or keeping business. Outside counsel can assist not only in interpreting complex and changing regulation but also in advising on best practices that are emerging across a wide range of industries. The following areas are just some of the regulations that may impact a business.

SARBANES-OXLEY

SOX provides for enhanced financial disclosures for public companies and mandates improved corporate governance practices. In addition, many of the provisions of SOX regulate the conduct of officers and directors. For example:

- Section 402 bans public companies from making loans to its officers and directors.
- Section 403 shortens the due dates for insiders (officers, directors and 10% shareholders) to publicly report transactions in their company stock to two business days.
- Section 304 requires a public company's CEO and CFO to disgorge any bonus and other incentive or equity based compensation received during the previous 12-month period in the event that the company has to restate its financial statements due to any material non-compliance or misconduct under the reporting requirements of the federal securities laws.
- Section 306 and newly adopted SEC rules prohibit public company officers and directors from making transactions in the company's stock during pension fund "blackout" periods.

Many of the provisions of SOX and related corporate governance rules also overlap with the elements and provisions of an effective compliance program. These new provisions and rules from SOX join existing legislation and regulations that protect shareholders and other stakeholders from corporate misconduct. Accordingly, companies should consider the interaction of these overlapping activities and requirements when designing and implementing their compliance programs. Doing so will ensure that companies weave an effective "web" of corporate compliance. Without such a web to catch malfeasance, a company will be vulnerable to acts with the potential to terminate the organizations existence. Several of these key provisions are discussed below.

DISCLOSURE CONTROLS

Even before SOX was passed, the SEC required public companies to have a system of internal accounting controls in place. SOX builds upon this concept and creates new obligations in the corporate reporting process. Companies must now establish and maintain disclosures controls and procedures and prepare and disclose reports on the company's internal controls.

Under Section 302 of SOX, public company CEOs and CFOs must certify that they are responsible for establishing and maintaining "disclosure controls and procedures." This term encompasses a process by which all information that is responsive to financial and non-financial disclosure requirements is assembled, tested for quality and communicated to management (including the CEO and CFO), which then reviews the information before disclosing it in the company's periodic reports. The SEC recommends the formation of a Disclosure Committee comprised of persons responsible for accumulating information for, and preparing, public reports. The company must also review the disclosure controls and procedures and disclose management's conclusions about the their effectiveness in the company's quarterly reports (10-Qs). In addition, the company must disclose in its quarterly reports whether or not there were significant changes in the company's "internal controls" or in other factors that could significantly affect the internal controls, including any corrective actions with regard to significant deficiencies and material weaknesses.

INTERNAL CONTROL OVER FINANCIAL REPORTING

Under Section 404 of SOX, in the near future public companies will be required to include in their annual report an internal control report that includes information about the company's internal controls over financial reporting. The company's quarterly reports must also include an evaluation of any changes that have materially affected or are reasonably likely to materially affect the company's internal controls over financial reporting. "Internal controls over financial reporting" encompasses a process designed by, or under the supervision of, the company's principal executive and financial officers, and effected by the board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with GAAP. This process includes policies and procedures that:

- pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the company;
- provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with GAAP, and receipts and expenditures of the company are begin made only in accordance with authorizations of management and directors of the company; and
- provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements.

These policies and procedures are management functions. While the company's auditor must attest to, and report on, the management's assessment, they cannot perform these tasks for management (Section 302 of SOX prohibits the company's auditor from performing specified non-audit services).

THE COSO FRAMEWORK

Disclosure controls overlap and intersect with internal control over financial reporting. In any event, both are derived from, and share components with, the framework for internal controls set forth in the report by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The COSO framework is the most broadly accepted framework for internal controls that has come forth from the auditing profession and is especially helpful in designing, maintaining and evaluating internal controls and procedures for financial reporting and disclosure controls and procedures. Components of the COSO framework consist of five interrelated components:

(1) Control Environment. This is the foundation of the internal control system. It provides fundamental discipline and structure and sets the tone of the organization that influences the integrity, responsibility and ethical values of its employees.

(2) Risk Assessment. This identification and analysis of the risks of the company form the basis for determining how the company's risks should be managed.

(3) Control Activities. These are the policies, practices and procedures that help ensure that management objectives and risk mitigation strategies are achieved. This includes activities such as approval, authorization, verification, recommendation, asset security and segregation of duties.

(4) Information and Communication Systems. These systems ensure that pertinent information is identified and communicated to people so that they are able to carry out their responsibilities in a timely manner.

(5) Monitoring. There must be an assessment of the control system's performance over time. This should include ongoing monitoring activities or external evaluations or a combination of both.

A first step to implementing Section 404 is to analyze and document the internal controls that the company already has in place. Implementation of Section 404 systems should be coordinated with the company's existing disclosure controls and procedures and certification rules and provisions set forth in SOX. Existing controls should be enhanced and new internal controls established by examining the needs of the company and by using the COSO framework as a benchmark. Internal controls and effective disclosure controls and procedures are an essential element to an effective compliance program.

CODE OF ETHICAL CONDUCT

Section 406 of SOX requires public companies to disclose whether they have adopted a code of ethics for their principal executive and senior financial officers. If a company has not adopted a code of ethics, it must explain why it has not done so. Under the SEC requirements, the code of ethics is a collection of written standards that are reasonably necessary to deter wrongdoing and promote:

- Honest and ethical conduct;
- Accurate and timely disclosure in the company's public reports;
- Compliance with the law;
- Internal reporting of code violation; and
- Accountability for adherence to the code.

Public companies must make the code of ethics available to the public (either by filing it as an exhibit to its annual report, posting it on the company's website or undertaking to provide a copy to any person without charge upon request). In addition, the company must disclose changes to, or waivers from, its code of ethics. These rules are applicable to companies beginning with their annual reports for fiscal periods ending on or after July 15, 2003.

STOCK EXCHANGE GOVERNANCE REQUIREMENTS

In addition to SOX and new SEC rulemaking, the stock exchanges, such as the NYSE and Nasdaq, have proposed their own new corporate governance standards for companies who list securities with them. The SEC is expected to adopt these governance listing standards in final form in late October or early November. The new governance requirements will go into effect in 2004 and address the following topics:

- Director independence rules;
- Audit committee and other board committee composition and responsibilities;
- Director education and training requirements;
- Corporate governance guidelines; and
- Code of business conduct and ethics.

Companies that have securities listed on one of the national stock exchanges should review the new governance listing standards carefully in order to make sure they are integrated with the company's overall compliance program.

WHISTLEBLOWER PROVISIONS

One of the audit committee requirements that flow from Section 301 of SOX is the requirement that audit committees establish procedures for (1) the receipt, retention and treatment of complaints received by the company regarding accounting, internal accounting controls or auditing matters, and (2) the confidential, anonymous submission by employees of the company of concerns regarding questionable accounting or auditing matters. SOX and the final SEC rules do not mandate specific procedures.

SOX also has express provisions to protect whistleblowers. Section 806 of SOX provides that civil liability may be imposed on public companies that take retaliatory action against employees who come forward with information about actual or potential corporate fraud involving their employer. Employees seeking relief under this provisions must first file a complaint with the Department of Labor. In addition, Section 1107 of SOX provides for new criminal sanctions against persons who knowingly and intentionally retaliate against informants in federal investigations. There are also other whistleblower protection provisions set forth in other legislation, such as the False Claims Act).

Companies should consider how they will comply with the newly mandated complaint procedures. Whatever type of system is implemented, it must provide for true anonymity. People must feel secure that they are raising complaints in confidence (e.g., making complaints by telephone can run the risk of the listener recognizing the voice of the person making the complaint). Hotlines, e-mail or web-based systems should be developed so that the sender cannot be identified by the company. While the need for confidentiality is paramount, the system should also be designed so that the company has the ability to conduct a thorough investigation. This should include a mechanism for the company to follow up with the person (on an confidential basis) who initially submitted the complaint.

Who should receive the complaints? Because of the potential for immaterial or spurious complaints, it may be beneficial for someone to screen the complaints before they are forwarded on to the audit committee. This screener could be an internal compliance or legal officer or a third party. The screening procedures should be reasoned and well thought out and the audit committee should have the ultimate authority to review any complaint or screening decision. Companies must also notify

employees of the existence of the complaint reporting system. The communication should encourage employees to report any perceived wrongdoing and not just merely advise them that the system is available. Communication of the system should be made on a regular basis, instead of merely a one-time notification.

U.S. FEDERAL SENTENCING GUIDELINES

The organizational sentencing provisions of the U.S. Federal Sentencing Guidelines (the "***Guidelines***") help courts determine the appropriate sentence for companies convicted of a federal crime. Interestingly, the Guidelines is one of the few publications that offers some specific and practical guidance as to what is required of an effective compliance program. The Guidelines impose significantly lighter penalties on companies that adopt and follow an effective compliance program. The Guidelines list seven elements for an effective compliance program:

1) Established compliance standards and procedures that help reduce the prospect of criminal conduct;
2) Oversight by high-level managers;
3) Due care in delegating authority to employees;
4) Effective communication of standards and procedures to all employees;
5) Monitoring and auditing systems and reporting mechanisms;
6) Enforcement of disciplinary mechanisms; and
7) Appropriate responses by the organization after detection of violations, including any necessary modifications to the compliance program.

The Guidelines aren't just for public companies—they apply to private and public companies of any size. The Guidelines also recognize that compliance programs are not one-size-fits-all. An effective compliance program will reflect the culture of the organization, as well as its size, business risks, complexity, industry, history and geographic scope.

Provisions of SOX enhance or increase penalties under existing criminal statutes and call for amendments to the Guidelines. For example, Section 903 of SOX increases the maximum penalties for mail and wire fraud from five years to 20 years' imprisonment and Section 1107 of SOX amends the Securities Exchange Act of 1934 to raise the maximum corporate fine for securities law violations from $2.5 million to $25 million.

In response to these directives, the U.S. Sentencing Commission implemented amendments to the Guidelines effective January 25, 2003. In addition, on January 20, 2003, the Department of Justice issued revised Principles of Federal Prosecution of Business Organizations to make clear that the existence and adequacy of a company's compliance program is an important consideration in determining whether to prosecute a company.

ATTORNEY PROFESSIONAL RESPONSIBILITY

Pursuant to Section 307 of SOX the SEC adopted rules that establish standards of professional conduct for attorneys who appear and practice before the SEC. Under these new requirements attorneys who appear and practice before the SEC on behalf of public companies (including in-house and outside attorneys) are required to report evidence of a material violation of securities laws or

breach of fiduciary duty or similar violation by the company or its agents to the company's chief legal officer (**CLO**) or chief executive officer (**CEO**). The officer receiving such a report is required to conduct an inquiry, take appropriate remedial action if warranted, and report back to the attorney who submitted the initial report. If the reporting attorney does not receive an appropriate response, then the attorney must report "up the ladder" within the company, to a committee of independent directors or even to the entire board itself.

In lieu of attorneys reporting material violations to the CLO and/or CEO, companies have the option of establishing qualified legal compliance committees (**QLCCs**) to receive, investigate and respond to reports from attorneys. One advantage to establishing a QLCC is that the reporting attorney is not required to assess the company's response to the reported evidence of a material violation. QLCCs must adopt written procedures for the confidential receipt, retention and consideration of any report of evidence of a material violation.

Whether a company has established a QLCC or not, an effective compliance program for public companies must provide for an internal reporting system that meets the specific requirements for attorneys practicing before the SEC. Procedures should be devised based on the company's culture, structure and needs and the size of its legal staff.

DOCUMENT RETENTION POLICIES

A document retention or management policy is a set of guidelines devised to control the amount of time documents are retained before they are destroyed or disposed of. An effective document retention policy has two primary benefits. First, it helps meet the company's operating needs by providing efficient and economic storage and location of records. Second, it helps meet certain legally mandated records retention procedures as discussed more fully below.

Certain laws mandate minimum time periods for which records must be retained. The specific time requirements depend on the state in which the company does business and the differing state and federal laws and regulations applicable to the business of the company. Another important purpose of any document retention policy is to avoid problems once a lawsuit (or other proceeding) has been threatened or filed against the company. If evidence is found to have been improperly destroyed in the context of a lawsuit or investigation (referred to as spoliation), then a court, among other things, may instruct the jury that negative inferences can be made as a result of such destruction (i.e., that the evidence was damaging to the company). Companies can avoid this negative inference instruction by demonstrating that records were destroyed in conformance with a proper document retention policy. Courts have ruled that a proper destruction program is one which (i) is not instituted in bad faith; (ii) is not selectively applied and (iii) incorporates retention periods which are reasonable (i.e., based upon proper legal research).

The Arthur Andersen/Enron document shredding fiasco, which illustrates that obstruction of justice charges can result from the destruction of documents even before a company receives a subpoena or other formal notice of an investigation, was the driving force for some of the provisions in SOX. Section 1102 of SOX makes it a crime punishable by up to 20 years imprisonment to tamper with records or otherwise impede an official proceeding. Similarly, Section 802 creates two new criminal sections pertaining to the destruction of records.

In light of the new obstruction provisions and prosecutors inclination to use them as the basis for pursuing perceived wrongdoing, companies should revisit their document retention policies to make

sure they are integrated with the compliance program and that all employees clearly understand their responsibilities in carrying out the policy.

THE PROLIFERATION OF ELECTRONIC DOCUMENTS

Even assuming that a company has adopted (and more importantly, implemented) an adequate document retention policy, in today's environment, the chances are good that, at some point, the company will have to review the documents it has retained either in response to a governmental investigation, its own internal investigation or to litigation. More than ever before, electronic documents have been identified as playing a crucial role in all these types of circumstances.

Just as advances in technology have changed the way we do business, these same advances have changed the way companies must think about the way in which they retain and manage their documents. More than 93 percent of today's corporate documents are electronic, and many of those are never printed to paper. Perhaps the most notable difference between today's electronic environment and paper environment of the past is volume. The ease with which employees can create, duplicate, distribute, and store electronic documents means the volume of relevant electronic material a company has is usually much greater than the volume of paper. Cheap storage is a major culprit here. A standard compact disk can hold approximately 325,000 pages of documents – or about 100 banker's boxes of material. A typical desktop computer may have a 20 to 40 gigabyte hard drive – representing a storage capacity of 1 to 2 million pages! Two million printed pages would fill roughly 600 banker's boxes, requiring a separate facility to store them all. In the world of electronic documents, however, this storage facility of boxes fits neatly on your desktop. Given the tremendous storage capacity available, the average computer user has little incentive to purge and delete files.

Another important characteristic of electronic documents is their dynamic nature. They are easily created, and easily altered. As a result, the realm of electronic documents has introduced new forms of evidence that simply did not exist in the traditional hard-copy document realm. For example, phone conversations that often involved no discoverable documentation have largely been replaced by electronically memorialized communications such as email and instant messaging transcripts. In addition, deleted documents, draft documents that were never printed to paper, unsent emails, and documents that were never saved may still exist on a user's hard drive. Finally, electronic documents contain a wealth of information that "disappears" when the document is converted to hard copy. Examples include hidden comments viewable only in the electronic version of a document, or the metadata attached to an electronic document, which reveals information such as when the document was last edited, and by whom.

The flexibility and transferability that make electronic documents so popular creates a number of complications for reviewing and producing those documents in an investigatory context. Because electronic documents are so easily manipulated, duplicated, and transferred, there are many more potential locations and sources of responsive material. When an employee has documents spread among several sources, such as the hard drives of desktop computers, file servers, laptops, floppy disks or CD-ROMs, finding and collecting all potentially responsive documents can be a challenge. Not only may it take more time to identify all the storage places for the documents, but also it may take considerable resources to gather these documents into a usable format. For example, retrieval of data from backup media may require special programming both to restore, and to convert, the data into a form that can be read by an opposing party. Frequently, the hardware required to upload old backup tapes may be obsolete and/or impossible to obtain. As a result, collection of deleted or other residual data from a hard drive or other storage media may require the services of a computer forensics expert.

From the company's standpoint, electronic document discovery can be both a blessing and a curse. The cost of duplication, shipping, and storage for documents produced in electronic form is much less than when produced in paper form. In addition, technology begets technology. Some of the disadvantages created by the volume of electronic material are offset by the ability to quickly search and sort documents electronically. Advanced technology allows one to further manage electronic documents by identifying and suppressing duplicate files. In addition, loading documents into a litigation support system is much less expensive and time consuming if the documents already exist in electronic format. On the other hand, even with the development of technologies to assist in electronic data management, the incredible increase in volume experienced by many companies causes more than its fair share of problems.

In light of the ever increasing volumes of electronic documents and the reporting requirements of SOX, companies should carefully explore the various technologies and services designed to assist them in reviewing significant volumes of both electronic and paper documents to identify, investigate and hopefully remedy potential violations before they get out of control.

PRIVACY AND SECURITY OBLIGATIONS

A company's failure to adequately secure and protect its information systems could subject the company to lawsuits and regulatory proceedings, not to mention loss of business reputation, etc. The company's privacy and security policy and procedures are important elements of the company's overall compliance program. As such, they should be integrated with the company's document retention policies and overall risk management and regulatory compliance policies and procedures. In designing and implementing privacy and security policies and procedures, companies should be aware of the myriad of privacy and security laws that the company may be subject to.

Gramm-Leach-Bliley Act. GLB requires financial institutions, which are deemed to include banks, insurance companies, finance companies, retailers providing credit services, and financial/investment/economic/tax advisors, to safeguard all "personal nonpublic information" of consumers and customers. It also requires the provision of privacy notices to consumers, and allows consumers, with certain exceptions, to choose whether their financial institutions may share their information with third parties. The Federal Trade Commission ("FTC") has the authority to undertake enforcement actions to ensure that financial institutions comply with the law.

Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). HIPPA requires healthcare organizations to safeguard "individually identifiable health information" of patents and enrollees.

Federal Trade Commission. The FTC regulates against "deceptive practices" relating to how companies collect, use and secure consumers' personal information. The FTC also protects consumer privacy under the Fair Credit Reporting Act and the Children's Online Privacy Protection Act and other federal statutes.

California SB 1365. Effective July 1, 2003, California revised its business laws to require notification of customers if a "security breach" leads to the disclosure of a customer's unencrypted personal data. This law applies to any person or company that conducts business in California and stores personal information about its residents on computers, regardless of whether the person or company has an office or computers in California.

These laws highlight the importance of companies maintaining privacy and security policy and procedures that include audit and training functions as well as providing notification in the event of unauthorized disclosure. An effective security solution requires a combined understanding of all of the relevant technical, business and legal issues.

A FLY IN THE WEB: RESPONDING TO A CRIMINAL INVESTIGATION

For most companies, when it becomes apparent that a criminal investigation is underway, or possible, the only realistic alternative is to retain outside counsel who is experienced with handling criminal investigations of so-called business crime, but more often, crimes that relate to a company's relationship with the state or federal government and their agencies. Nevertheless, there are some consistent mistakes companies make when responding to criminal investigations, and some consistent approaches for companies that "successfully" ride them out.

The first rule: don't make your situation worse by attempting—improperly—to keep information from the government, or by offering information to the government unless that strategy has been carefully—but quickly—thought through with counsel and all relevant departments. No matter what else your company does in response to a criminal investigation, you will be far better off if you make no attempt to—put it bluntly—lie, or give the impression that you are lying. If you are going to talk—and that is a big if—whatever you do, tell the truth. You can rarely go wrong by remaining silent until everything can be properly sorted out with counsel, but talking, attempting to minimize your culpability and certainly, doing anything that will give the impression that you are being anything other than completely honest, will worsen the company's situation in two important ways. First, you will be committing new crimes. We very often see instances where the underlying crimes being investigated were not provable—in other words, we had a very "triable" case--only to learn that a misguided employee—whose actions will be attributed to the company under the law—altered (often they will say "corrected") a document, or submitted to an interview and did not tell the truth. Often these things are done in some early phase of an investigation which was not criminal when it started, but becomes so after the "ancillary misconduct" occurs, often leading to search warrants and other extraordinary investigative means. In addition to creating new crimes, such misconduct makes it difficult to convince a jury that the company did nothing wrong and had nothing to hide. This, in turn, makes it difficult to head off an indictment or otherwise achieve a favorable result.

Second, it is important to obtain qualified outside counsel and auditors, if necessary, to investigate potential criminal matters quickly. It is important to get out in front of the investigation and see what the company is facing before deciding on a course of action. Using outside counsel to do this will make it easier to protect attorney client privileges and work product—to the extent that is still possible at all—and give your disclosures to the government, if you decide to make them—a greater appearance of independence and objectivity.

Finally, companies that survive criminal investigations with their business intact, demonstrate at all times that they "have religion"—that is, they take the matter seriously. The typical corporate client and its managers, are tempted to view the government's investigation as frivolous nitpicking. Often they feel singled out—and sometimes they are. Even though the company may feel that way, it is best not to give the government the impression that you are not taking its investigation seriously. We are continually confronted with cases that we cannot believe are being pursued by the prosecutors and cases that we cannot believe are not, but no matter upon which end of that "luck of the draw" you end, you always want to give the impression to the government that you take its inquiry seriously and that you are a good corporate citizen.

CONCLUSIONS

The question of whether or not to implement a compliance program is no longer to be debated. Companies must adopt effective and comprehensive compliance programs that are specifically tailored to their individual business needs. In the current environment, companies with a "head in the sand" mentality are at risk; prosecutors and regulatory organizations are "loaded for ostrich." As a result, implementation of effective compliance program is emerging as a "best practice" for all companies. To be sure, this requires the allocation of additional budgetary resources in tight economic times. However, the costs of compliance are far outweighed by the costs of non-compliance. Finally, beyond the dollars and cents, studies indicate that employees of companies with a strong culture of ethics and compliance have higher levels of job satisfaction, feel more valued, and are more loyal to their company than employees at companies where compliance and ethics are not emphasized. Is your company's web of compliance in place?

Preston Gates & Ellis has been providing private and public sector clients with counsel, litigation, legislative advocacy and transactional services for more than 120 years. As a full-service law firm we offer over 400 attorneys and professional staff in nine cities throughout the West Coast, in Washington, D.C. and in Hong Kong.

Our lawyers and professionals believe in working as a team with our clients and each other. We make extensive use of sophisticated communications, document production and research technology, and stand ready to meet all of our clients' legal needs, from drafting simple documents to coordinating major multi-party transactions throughout the United States and the world.

Preston Gates professionals practice in 40+ areas of law including business, employment & labor, environmental and land use, litigation, municipal, real estate & finance, technology & intellectual property, public policy

DATG is a practice group within Preston Gates & Ellis LLP, dedicated to providing clients with efficient document review legal services. This group of experienced professionals uses specialized processes and advanced technology to provide quality document review legal services, while saving clients significant time and money in many cases.

*For more information please visit **www.prestongates.com** or contact one of four attorneys listed below:*

Julie Anne Halter, jhalter@prestongates.com, (206) 623-7580
Gary J. Kocher, garyk@prestongates.com, (206) 370-7809
Daniel Marino, dmarino@prestongates.com; (202) 661-3805
Chris K. Visser, cvisser@prestongates.com; (206) 370-8343