Chief Executive
RESEARCH

Chief Executive Legal Guide

1 Sound Shore Drive, Suite 100, Greenwich, CT 06830
Telephone: (203) 930-2700 · Fax: (203) 930-2701
www.chiefexecutive.net/research

Marshall Cooper: Chief Executive Officer

Wayne Cooper: Chairman

David Beck: Senior Vice President

Michael Bamberger: Vice President of Research

Chris Horner: Editor

Elayne Demby: Editor

Paula Santonocito: Editor

Monique Nijhout: Desktop Editor

CHAPTER 1

WHITE COLLAR CRIMINAL LAW

Gibson, Dunn & Crutcher LLP

Criminal Investigation & Liability
Marcellus A. McRae, Partner
Tzung-Lin Fu, Associate

Personal Criminal Liability of CEOs
Marcellus A. McRae, Partner
Daniel L. Weiss, Associate

Securities Fraud
George H. Brown, Partner

Foreign Corrupt Practices Act
Jim Walden, Partner
Daniel J. Chirlin, Associate
Stephenie Gosnell Handler, Associate
Kacie A. Lally, Associate

Data Privacy
Debra Wong Yang, Partner
Justin S. Liu, Associate
Meredith A. Smith, Associate
Susannah Stroud Wright, Associate

INTRODUCTION

The stakes are high in white collar criminal matters. Your company can be subject to severe penalties such as fines, disgorgement, and onerous remedial and compliance requirements. Moreover, employees and officers can be held personally liable and possibly face prison sentences. As the CEO, you may be personally prosecuted for not only your own actions, but also the actions of other employees even if you did not know about or participate in the criminal activity. Even if the criminal allegations are not ultimately substantiated, the mere fact that your company or you have come under criminal investigation can lead to regulatory enforcement actions and shareholder lawsuits, and hurt the company's reputation and bottom line.

Criminal liability may arise from failure to comply with various federal and state laws. For example, misleading or inaccurate financial statements can evolve into a securities fraud prosecution. Willful violations of securities laws can create criminal exposure for both the company and its officers. If your company has overseas transactions, it may also be at risk of violating the Foreign Corrupt Practices Act. The Act creates civil and criminal liability for giving anything of value to foreign officials to obtain or retain business, failing to keep accurate books and records, and failing to develop and maintain reasonable internal controls.

A criminal issue may arise from a government investigation brought by federal or state prosecutors, but it may also come to your attention before the government becomes involved. Either way, it is important to conduct a swift and thorough investigation so the company can understand the facts and take appropriate actions to mitigate its potential criminal exposure. The investigation may be complicated by foreign and domestic data privacy laws imposing restrictions on the collection, transfer, or processing of data. Experienced counsel can help you navigate these complex data privacy issues.

Counsel can also help you assess your company's exposure and determine the best response to the situation. If the government has not yet become involved, counsel can help you decide whether to voluntarily disclose the issue to the government. If a government investigation is already under way, experienced criminal counsel can help persuade the government not to formally prosecute the company or its employees, reach a favorable settlement or plea deal, or mitigate the company's exposure in other ways.

Don't forget that a strong compliance program can be your best insurance against criminal liability. A good day-to-day compliance program can help prevent criminal misconduct from happening and allow the company to detect any potential problems quickly. If your company comes under government scrutiny, the government may view a robust compliance program as a mitigating factor in considering whether to prosecute.

PART I. CRIMINAL INVESTIGATION & PROSECUTION

A. WHAT IS AT STAKE

A company under criminal investigation or prosecution faces not only possible fines, disgorgement, onerous remedial and compliance requirements, monitors, and jail time for responsible officers and employees, but also collateral consequences such as civil and administrative enforcement actions brought by government regulators, and civil suits brought by shareholders. Moreover, the mere fact that the company is under criminal investigation may cause substantial loss of stock value, reputation, and good will, even if no criminal liability is ultimately substantiated.

This chapter will give you a brief description of the criminal process and the various theories under which a CEO can be held criminally liable in his or her personal capacity. It will then discuss two areas of law that have seen active prosecution in recent years: securities fraud and the Foreign Corrupt Practices Act. And finally, it will provide you with an overview of domestic and foreign data privacy laws that you may encounter in criminal investigations, government enforcement actions, and even civil litigations and day-to-day operations of your company.

B. ANATOMY OF A WHITE COLLAR CRIMINAL PROSECUTION

Internal Investigation. Sometimes, wrongdoing inside your company may come to your attention before any prosecutor ever learns of it. The issue may surface from a routine financial audit, an internal whistleblower report, or a tip from your supplier. Whatever the source, consider yourself lucky for hearing about the problem first, and take immediate action to conduct a swift, thorough, honest, and well-documented internal investigation.

It is a good idea to engage an experienced outside counsel to lead the investigation, or at least to advise on the risk exposure for the company and its officers, and whether any further steps should be taken. For example, if the investigation reveals that serious criminal misconduct in fact took place, and that the government is likely to independently learn of the misconduct, your company may wish to voluntarily disclose the problem to the government, in the hope of receiving lenient treatment for being cooperative.

A good outside counsel can also advise you on what remedial measures may be needed to prevent future misconduct of a similar kind, or whether the problem is significant enough to require disclosure in your company's regulatory filings.

Government Investigation. Sometimes, a government investigation catches you by surprise. Perhaps some FBI agents just showed up at one of your company's facilities to execute a search warrant, to talk to your employees, or to look through your company's files. Maybe the Department of Justice just sent your company a voluntary request for documents. Or perhaps

someone in your company has received a subpoena to testify before a grand jury. Any of the above would likely suggest that a federal or state prosecutor has already been investigating your company for weeks or months.

Once you have confirmed the existence of the investigation, you will want counsel to immediately determine your company's investigation status in the government's eyes. For instance, your company may be a "target" of the investigation—a putative criminal defendant who is linked to the commission of a crime with substantial evidence. Or, your company could be a "subject" whose conduct is within the scope of the investigation. Alternatively, the government may view your company as a mere "witness" to certain facts.

These status determinations may have tremendous significance in terms of your company's potential liability exposure, financial disclosure responsibilities, and ability to operate without significant disruption. In addition to assisting the company in determining its status, experienced counsel at this critical juncture can help the company try to determine the focus and goals of the government's investigation.

If your company is the target of a government investigation, it is wise to quickly get a handle on the facts internally, and simultaneously start engaging the prosecutor through your criminal counsel to maximize the opportunity to: (i) present the company in the best possible light, and (ii) avoid criminal prosecution.

Charging Decision. If your company has been investigated, the government will ultimately decide whether or not to charge your company with any crimes. The decision may be based on a number of factors, including:

- How much evidence the prosecutor has against your company;
- How likely the prosecutor is to secure a conviction at trial;
- How well a criminal conviction may serve to deter your company and others from committing the same crime;
- The nature and seriousness of the offense;
- How pervasive the misconduct is within your company;
- Your company's history of similar misconduct;
- Your company's voluntary disclosure of the misconduct and cooperation in the investigation;
- The existence and effectiveness of your company's pre-existing compliance program;
- Any remedial actions your company has undertaken;
- Collateral consequences of charging your company, such as the possibility of causing disproportionate harm to the company's shareholders or employees;

- The adequacy of prosecuting the responsible individuals (as opposed to the company); and
- The adequacy of civil or regulatory enforcement actions or other remedies.

The company's goal is to obtain a decision not to prosecute (a declination) from the government. If that fails, companies often seek to resolve potential criminal charges by entering into non-prosecution agreements ("NPAs") or deferred prosecution agreements ("DPAs") with corporate targets.

Both types of agreements are predicated on a set of conditions, which may include substantial fines, disgorgement, and a host of possible remediation and compliance conditions. With an NPA, the government agrees not to prosecute the company as long as it complies with the terms of the agreement. With a DPA, the prosecution typically files criminal charges in court, but waits for a certain amount of time to decide whether or not to prosecute the case, depending on whether the company has complied with the terms of the agreement.

If the government decides to bring criminal charges, a criminal complaint or indictment is filed, setting out the allegations against the corporate defendant and the crime(s) it is accused of committing, and the prosecution proceeds before a state or federal court.

Plea Bargaining. After charges are filed and a criminal case is commenced in court, there is a further opportunity to settle with the prosecution through plea bargaining. This typically involves the corporate defendant pleading guilty to one or more of the charges, in exchange for the prosecutor's agreement to drop certain other charges or recommend lighter sentences to the court. If your company decides to plead "not guilty" to the pending charges, the case proceeds to trial.

Criminal Trial. A corporate criminal defendant has the same right to be tried by a jury as an individual defendant. At trial, the State or the United States, represented by the prosecutor, plays the role equivalent to a civil plaintiff, and presents its evidence to convince the judge or jury that your company should be found guilty of the charges beyond a reasonable doubt. Your company, as the defendant, will present its evidence to show that it is not guilty. At the end of the trial, the jury will determine whether your company should be convicted of each of the charges brought against it.

Sentencing. If the company is found guilty of one or more charges, it will be sentenced by the judge, who will rely on the criminal statutes and a set of discretionary sentencing guidelines to calculate the appropriate penalties. While a company is considered a legal person for purposes of charging it with a crime, it is not subject to imprisonment, nor is an officer of the company imprisoned on behalf of the corporate defendant. Thus, the sentencing of a corporate defendant usually includes fines and disgorgement. Corporate officers convicted in their individual capacities, however, may face prison time. The sentence may be reduced or enhanced based on factors such as substantial assistance to authorities or obstruction of justice.

C. CEO ACTION PLAN

Because the stakes are high in a criminal case, the right response to a criminal investigation or prosecution is critical. Here are a few things you can do as a CEO:

Hire Experienced Counsel. Because the stakes are high in a criminal case, you want to make sure your company's interests are protected in every step of the process. A good white collar criminal defense counsel can help you conduct a thorough internal investigation that will be credible to the prosecutor, help persuade the prosecutor that your company either should not be charged or should be treated more leniently, and defend your company through the court process.

Among other things, he or she can: (i) warn you against pitfalls in the process; (ii) help weigh the pros and cons of different approaches (such as whether to voluntarily disclose internally discovered misconduct or to accept a plea offer); and (iii) take the lead on dealing with the legal process, allowing you and your staff to spend more time on the business during what is invariably a stressful time for everyone in the company.

Also, don't forget that communication between a lawyer and his or her client can be protected from disclosure by the attorney-client privilege. If the privilege applies, this means you and your company can consult with your counsel in confidence on the legal issues, and the contents of your discussions generally will not need to be revealed in court.

Preserve Documents and Protect Whistleblowers. As hard as it is for your company to be subject to a criminal investigation or prosecution, being accused of obstruction of justice personally can be worse, as it can lead to charges against you personally and enhanced sentences for both you and your company (which may be vicariously liable for your conduct) if you are found guilty.

To prevent this, use your best efforts to ensure that all documents and evidence that may be relevant to the investigation or discoverable are preserved as soon as you learn of a potential criminal investigation. Similarly, if a company employee reports wrongdoing internally or directly to the authorities, he or she should be protected from termination or any other adverse actions that may be interpreted as retaliation.

Conduct a Swift and Thorough Internal Investigation. Knowledge is power. When potential criminal misconduct surfaces in your company, immediately conducting a comprehensive investigation will allow you and your lawyer to get on top of the facts, assess the company's potential exposure, and decide on the best response to the situation.

In addition, if you decide to voluntarily disclose the issue to the government, or if the government already knew of the problem before you were aware of it, being able to share the findings of a timely and credible internal investigation will not only show that your company takes responsibility for its wrongs, it may give you additional bargaining chips with the prosecution when negotiating leniency or a NPA, DPA, or a plea agreement.

Manage Your Public Relations Message. A criminal investigation or prosecution can be devastating to the public image and value of your company. While you may not be able to prevent public knowledge of the existence of the investigation, you can often help shape the message the public hears about the investigation, and thus mitigate the impact to your company. Be sure to involve your legal team in your PR strategy. The last thing you want to do is make a public statement that would hurt your court case or enrage the prosecution.

Strengthen Your Compliance Program. Like so many things in life, prevention is better than reaction. Having a strong day-to-day compliance program can help prevent criminal misconduct from happening in the first place. When potential misconduct occurs, a good compliance program may help the company detect the problem quickly, enabling the company to take appropriate actions to mitigate the risk of a criminal investigation and prosecution.

In addition, as mentioned before, the government may view a robust compliance program as a mitigating factor in considering whether to prosecute. Even if your company did not previously have a strong compliance program, establishing one now will show that your company cares about doing the right thing, takes responsibility to redress past problems and prevent future ones, and should be treated more leniently.

PART II. PERSONAL CRIMINAL LIABILITY OF CEOS

A. WHAT IS AT STAKE

CEOs are not immune from criminal prosecution in their individual capacity for acts committed in the scope of their employment. In fact, in certain circumstances, CEOs can be personally liable for the actions of other officers and employees even if the CEO did not have knowledge of and did not participate in any manner in the criminal activity.

It should come as little surprise that the penalties and ramifications for a CEO who is convicted personally of a crime are significant. The penalties stemming from a criminal conviction could include:

- Incarceration;
- Probation;
- Monetary fines and penalties;
- Restitution; and
- Forfeiture of ill-gotten gains, including compensation and other benefits provided by the company to the CEO.

Aside from the specific criminal penalties, CEOs who are convicted of a crime could potentially face a number of other collateral but noteworthy consequences, including:

- Exclusion from state and federally regulated industries, such as financial, security and healthcare;
- Revocation or suspension of state and federally issued licenses;
- Personal civil liability; and
- Disruption of private and professional life.

This section is intended to provide you with a high-level overview of the means through which you, and other officers, could be personally liable for criminal violations.

B. THE VARIOUS MEANS THROUGH WHICH A CEO CAN BE PERSONALLY LIABLE FOR CRIMINAL VIOLATIONS

Generally, establishing that a person is guilty of a crime requires the government to prove two fundamental elements: (1) a wrongful act (e.g., theft); and (2) a culpable state of mind (e.g., intent to steal). However, there are criminal statutes that do not require a culpable state of mind but only require that the government establish a wrongful act—these are defined as strict liability crimes. There are also criminal statutes that hold a person responsible for the

acts of a third party even if the person did not participate in or have knowledge of the third party's conduct, which are known as vicarious liability crimes.

While there are relatively few strict liability and vicarious liability criminal statutes, as a CEO you are particularly exposed to personal criminal liability based on these types of statutes because they are often created to regulate business activities.

The Corporate Veil May Not Protect You

A well-known concept in corporate law is the corporate veil, which treats the corporation as a legal person that is separate from its shareholders, directors and officers. As a result, a corporation's shareholders, directors and officers are generally protected from being personally liable for the conduct of the corporation. Thus, because of the corporate veil, you are generally not personally held responsible for the actions of others within the company.

It is imperative to understand, however, that the corporate veil does not protect directors, officers, or employees who commit, participate in, or are otherwise involved in the commission of a crime from being personally prosecuted for their conduct. Thus, a CEO who engages in conduct that violates a criminal statute, e.g., securities fraud, can be prosecuted individually for his or her conduct. For this reason, it is not a defense to personal liability to assert that the criminal activity was in the scope of the CEO's employment or "for the benefit of the company," or that the company could also be held responsible for the criminal activity.

In situations when the corporate veil protects a CEO from criminal liability based on the actions of others within the company, a CEO may nonetheless be exposed to personal criminal liability if the government successfully pierces the corporate veil—lifting the distinction between the corporation and the officers. Although requirements differ by jurisdiction, to pierce the corporate veil, the government generally needs to demonstrate that the shareholders, directors, or officers disregarded the corporate formalities or used the corporate form to engage in a fraud or commit another injustice.

Accomplice Liability And Willful Blindness

Even if a CEO does not directly commit the criminal activity, if the CEO assists or encourages a co-worker or subordinate to commit a crime, he or she can be held personally liable under an accomplice theory. For instance, if a CEO directs a subordinate to engage in conduct that constitutes securities fraud, the CEO and the person or persons who committed the criminal activity may be personally liable for the criminal activity.

This accomplice theory of personal criminal liability is also applied in situations when a CEO or another supervisor obtains knowledge of a subordinate's criminal activity but does nothing to stop it. Further, accomplice liability may apply, even in the absence of knowledge, if the CEO is found to have looked the other way and was willfully or deliberately ignorant of his or her subordinate's criminal activities.

Execution of Certifications

CEOs may also face potential personal criminal liability arising from executing certifications that are later proved to be false. For instance, many regulatory statutes require a CEO, or other high-level executives, to certify, often under the penalty of perjury, that certain business activities or reports are true and accurate.

The most notable regulation over the last few years that requires this type of certification is the Corporate Auditing and Accountability Act of 2002, better known as Sarbanes-Oxley. Under Sarbanes-Oxley, CEOs and CFOs are required to provide personal certifications as to the truth of the corporation's quarterly and annual reports. If the certification is later proved to be false and the CEO knowingly executed the false certification, the CEO could potentially face personal criminal liability.

Responsible Corporate Officer

As set forth above, CEOs are generally exposed to personal criminal liability only for actions in which they personally engaged. However, in a limited (but increasing) number of situations, a CEO can be personally liable for criminal activity committed by other officers and directors.

For instance, the "Responsible Corporate Officer" doctrine provides that an executive may be personally liable for criminal violations that affect public health and well-being (e.g., health care and environmental regulations) in which he or she did not participate if the executive: (1) had direct control or supervision over the activity, or (2) was in a position to prevent the criminal activity.

It is critical to understand that the CEO need not have actual knowledge of or participation in the criminal activity—just having the authority to exercise control over the situation that led to the criminal violation is enough.

The Responsible Corporate Officer doctrine, however, does not apply if an executive can establish that it was "objectively impossible" to stop or correct the alleged violation or that he or she was powerless to do so. In some jurisdictions, courts have held that the Responsible Corporate Officer doctrine should not apply if an executive acted with "extraordinary care." These defenses are not well developed, however.

Case Study: The CEO of a national food chain was personally charged, along with the company, with a violation of the Food, Drug, and Cosmetic Act after the government repeatedly notified the company that it found rodent contamination at the company's food-storage warehouse. Despite not being involved in the alleged criminal violation, the CEO was convicted because he was in a position and had the responsibility and authority to prevent the violation or to promptly correct it. See United States v. Park, 421 U.S. 658 (1975).

C. CEO ACTION PLAN

Know the Law. Because CEOs are not immune from personal criminal liability, you must become familiar with the criminal statutes that might be implicated by your business activities. State and federal criminal statutory schemes are broad and expansive, and while many of the statutes are directed at prohibiting inherently wrongful activity (e.g., money laundering or fraud), there are a number of other statutes and regulations that are less intuitive. It is these lesser-known statutes that can create peril for you, as ignorance of the law is not a defense.

Establish a Compliance Program. In addition, because in certain circumstances you are potentially exposed to criminal liability based on the acts of others within your company, you should coordinate with your internal and outside counsel to develop comprehensive compliance programs that deter employees from engaging in wrongdoing.

Further, because even the best compliance plan cannot deter all wrongful activity, you should implement sufficient controls and audits so that if any wrongdoing were to occur, you or your supervisors and managers could promptly identify such conduct. For example, you should implement guidelines regarding when an internal investigation should be instigated and who must participate in the internal investigation.

In connection with the company's controls and audits, you should ensure that internal processes are put in place that are directed at ensuring appropriate action is taken in response to any identified wrongful conduct. Critically, after the implementation of the compliance program and the controls and audit processes, you should continue to be actively involved in the compliance process.

Plan Ahead. CEOs also should coordinate with their internal and outside counsel to develop crisis management and other response protocols. Often, CEOs expose themselves to personal criminal liability not because they were involved in potential criminal misconduct but because they responded unlawfully once that misconduct came to light.

For instance, when allegations of potential wrongdoing against your company are made public, you may be tempted to contact customers, investors, or others to explain the allegations. However, your statements, if later proved to be false or misleading, may be the basis for a wire fraud or mail fraud charge against you. Likewise, your actions in response to discovering potential criminal wrongdoing may expose you to criminal liability for obstruction of justice and perjury, among other similar crimes.

Because you likely will be responsible for handling the initial response to the discovery of any significant criminal activity within your company, and taking the wrong steps may expose you to personal liability, it is a good idea to design a response plan well in advance of discovering any potential wrongful activity rather than address these issues for the first time during a period of great stress.

PART III. SECURITIES FRAUD

A. WHAT IS AT STAKE

The federal securities laws play a central role in the company's communications with its shareholders and other investors. The law requires complete and fair disclosures of information that would be important to a reasonable investor in making decisions about the company's stock and other securities. Statements by the company and its officers that are misleading or inaccurate can become subject to allegations of securities fraud and can trigger investigations by the United States Securities and Exchange Commission (SEC) and the Department of Justice (DOJ).

There are severe penalties that can be imposed on individuals and the company as a result of a successful government enforcement action. Willful violations create exposure to criminal fines and imprisonment. In addition, a significant investigation by the government can be very expensive to defend and may distract you and your management team from pursuing the company's business strategy and goals.

The SEC has continued to be aggressive in enforcing the securities laws and has initiated hundreds of enforcement actions in each of the past three years. In 2011, the SEC initiated over 700 enforcement actions, and more than 130 of those included a parallel criminal prosecution by the DOJ.

CEOs are regular targets of such actions. During 2011, several settled enforcement actions were announced involving CEOs in which the SEC used its authority under Sarbanes-Oxley and Dodd-Frank to require the CEO and other corporate officers to return incentive compensation paid during years where the company's financial statements were subsequently restated. CEOs and other officers are exposed to these "clawback" provisions, even in instances where they are not accused of wrongdoing.

B. LEGAL BRIEFING

The federal securities laws are designed to promote full and fair disclosures to the company's stockholders and investors in other securities of the company, such as bondholders or options purchasers. The primary statutes are the 1933 Securities Act and the 1934 Securities Exchange Act. The SEC is responsible for issuing rules and regulations to implement those laws and for enforcing them. Willful violations of the securities laws and regulations can also lead to criminal prosecution by the U.S. DOJ.

The federal securities laws and rules reflect a comprehensive set of requirements that tell companies exactly what must be disclosed when the company issues securities of any kind to the public, and imposes regular reporting requirements for those companies once any securities become registered with the Commission.

The Exchange Act also contains a broad anti-fraud provision that is the primary basis for challenges to misleading or inaccurate statements by the company or its officers. This law is known as Section 10(b) of the Exchange Act and is reinforced by the Commission's Rule 10b-5. Section 10(b) and Rule 10b-5 prohibit false and misleading statements and also cover other conduct such as insider trading.

Securities Fraud Based on False or Misleading Statements

The following are the elements that the U.S. Supreme Court has explained need to be proven in order to establish a violation of Section 10(b) based on false or misleading statements.

False or Misleading Statement of Fact. A statement can be characterized as false or misleading and become the subject of a securities fraud enforcement action in several ways:

- The company makes a statement that is literally untrue. For example, stating that: "We have significant new customer agreements in place" when the agreements are in fact not final, is inaccurate.
- The statement made is true, but misleading because important facts were left out. For example, stating that: "We have had exciting discussions about selling our product with several major potential customers," assuming it was actually true, could be misleading if it were also true that the majority of those potential customers had already rejected a proposed sale.
- The statement is an opinion not fact, but lacks a reasonable basis in fact or is not actually believed. Take for example, the statement: "Our goal is to close 10 major customer deals by the end of the second quarter." At the beginning of the fiscal year, this may be a perfectly reasonable explanation of the company's goals over the next six months, and would not be an "actionable" statement. However, if the same statement was made a few weeks before the close of the second quarter, and it is in fact unlikely that the company will achieve its goal of "closing 10 major deals," then the statement could be challenged as misleading under the securities laws.

Materiality. The alleged false or misleading statement must be material before it can be used to support a securities fraud enforcement action. A fact or omitted fact is material if there is a substantial likelihood that a reasonable shareholder would consider it important in making decisions about the company's stock or other securities. An omission that would be viewed by a reasonable shareholder as significantly altering the total mix of information available to investors about the security is considered material.

The SEC and the courts have explained that the materiality assessment is not simply a quantitative analysis, and that companies need to evaluate qualitative aspects of the contemplated disclosure when assessing whether it is material. For example, an error in the financial statements that is only 1% of total sales, but which swings the company's reported earnings from a profit to a loss, is potentially material. Despite what you might hear in informal settings,

there is no rule of thumb that says 5% is not material, and relying on a quantitative rule like that is very risky.

Case Study: In 2011 the U.S. Supreme Court decided a case involving disclosures by a manufacturer relating to its over-the-counter cold remedies. The product allegedly caused some individuals to lose their sense of smell. The number of reported adverse incidents was not statistically significant and the company argued that the failure to disclose those incidents could not be material under the law. The Court rejected the company's argument. Instead the Court repeated its previous position that no "bright line" rules should be drawn, and the question of materiality needs to be decided on the facts on a case-by-case basis.

State of Mind: the Scienter Requirement. A fraud allegation is a serious matter, and is not intended to apply to companies and officers who have made innocent or even careless mistakes. To establish a securities fraud claim, the government must show that the person making the statement had the intent to deceive, manipulate, or defraud investors. Courts explaining the requirement have generally agreed that a showing of severe recklessness satisfies the requirement, which is defined as misstatements or omissions that are not just careless or inexcusable, but reflect an extreme departure from the standards of ordinary care.

That said, a government investigation will focus on any and all facts that would suggest a motive to mislead investors, or that suggest that red flags about the true facts were known and not pursued. A CEO who continues to use a standard investor presentation over a period of time, without getting regular updates to ensure accuracy, would be subject to a claim of recklessness if the investor presentation is later alleged to have contained material inaccuracies.

Causation and Economic Harm. The government will have to prove that the misstatement actually caused economic harm to investors. There are two parts to the causation requirement:

1. First, there needs to be evidence that investors relied upon the false or misleading statement in connection with purchasing or selling the company's securities. In private securities class actions, the courts allow the case to proceed if the plaintiffs can show that the company's stock trades in an efficient market. The underlying premise is that an efficient market will rapidly incorporate into the stock price any material information that is available. Therefore, the law presumes that when false statements are made to the public in an efficient market there has been a "fraud-on-the-market" and the reliance component has been satisfied, unless the defendant can show otherwise.

For example, when a company announces earnings that exceed what the market had been anticipating, we typically expect the stock price in an efficient market to react quickly to that earnings surprise. If that earnings announcement is inaccurate, and overstates earnings, then the stock price will become distorted by incorrectly valuing the incorrect earnings. An investor who buys the stock in an efficient market has relied on the integrity of the market price as reflecting all available information, and this meets the first part of the causation analysis.

2. Second, there needs to be a showing that the false or misleading statement actually caused investors losses when the truth became known to investors and the stock price declined. This is referred to as "loss causation." The loss causation element requires a showing that inflation that was created by the original false or misleading statement was removed from the stock price as a result of the true facts becoming known to investors.

Using the above example, if the original announcement overstated earnings by ten cents per share, and the stock price was inflated by an extra $1.00, then when the truth comes out, that may cause the stock price to decline by $1.00. If that decline was in fact caused by the truth becoming known about the incorrect earnings, then the loss causation requirement has been met.

In practice, stock prices go up and down for a variety of reasons, and it is often very difficult to discern whether a correcting statement caused an investor to lose money, or whether some other event caused it. The analysis typically is done through the testimony of economic experts who conduct rigorous statistical analyses of the stock price reactions to the challenged and correcting statements.

Civil and Criminal Remedies for Securities Fraud

The SEC has numerous remedies available to it for a securities fraud violation. The SEC has its own administrative law judges and can bring an administrative action and obtain a "cease and desist" order prohibiting future violations. The SEC can also obtain administrative fines of up to $100,000 for individuals and $500,000 for companies.

The SEC can bring a civil action (non-criminal) in federal court and obtain a permanent injunction or fines. The SEC can also ask the court to issue a bar order preventing individuals from serving as an officer or director of a public company either temporarily or permanently. The civil fines can reach $100,000 for individuals and $500,000 for companies, but also can be increased to an amount equal to any gross pecuniary gain obtained as a result of the fraudulent conduct. In addition, for insider trading violations, the federal court can impose a fine of up to three times the improper gain obtained or loss avoided.

The SEC also has the authority to "claw back" prior incentive compensation paid to the CEO and other officers when there is a subsequent restatement of the financial statements. The law allows for such clawbacks even where there is no allegation of wrongdoing against the CEO or other officer.

Criminal fines and imprisonment for willful violations can be sought by the DOJ in a prosecution in federal court. The criminal fine can be as high as $5 million for individuals and $25 million for companies. Individuals can be sentenced to up to 20 years in prison after a conviction.

Securities Fraud Based on Insider Trading Allegations

An important goal of the federal securities laws is to promote fair and efficient capital markets. This goal is advanced in part by promoting equal access to information by market participants.

A perception by investors of unfairness in how stock prices behave, or that some market participants have an improper informational advantage regarding access to investment opportunities, undermines the legitimacy of our capital markets and could ultimately increase the cost of capital for companies raising money under such circumstances.

SEC Rule 10b-5 helps ensure that officers and other insiders do not gain an unfair advantage over investors by prohibiting insider trading. It is unlawful for any person to engage in the purchase or sale of securities while in possession of material non-public information about the company if they are an officer or employee of the company or are affiliated with the company in a way that gives them access to confidential non-public information and a corresponding duty to the company not to disclose it to others. This means that, in addition to company officers and employees, the law covers so-called "temporary insiders" such as the company's outside professionals, lawyers, accountants, and others who have an obligation to the company to protect the company's confidential information.

The law prohibiting insider trading also makes it illegal to disclose confidential information to persons outside of the company where it is likely that the information may be used in connection with the purchase or sale of the company's securities.

The SEC and DOJ actively and aggressively pursue insider-trading violations. Over the past few years there have been scores of enforcement actions and prosecutions, with a focus on the improper exchange of information between company insiders, hedge funds, and consultants. There are also many investigations that routinely arise out of trading activity in advance of company mergers and acquisitions.

C. CEO ACTION PLAN

If you are the CEO of a public company, you need to ensure that your management team and your outside professionals have implemented systems and procedures that will help the company avoid claims of securities fraud.

Here are several basic features that should exist in your company when you have SEC reporting obligations and public shareholders, regardless of how small your company may be:

- A Chief Financial Officer who has experience in financial reporting and SEC requirements for public companies.
- An Audit Committee of independent directors. The Audit Committee will need to meet NYSE or NASDAQ requirements, including having at least one person knowledgeable about financial reporting and Generally Accepted Accounting Principles ("GAAP").
- Internal Controls designed to provide reasonable assurance that material errors and/or fraud will be detected and corrected so that accurate financial reports can be prepared.
- An Investor Relations officer who is experienced with public company disclosure practices, and knowledgeable about the company's business.

- Legal review of all SEC filings and disclosures by counsel experienced in and knowledgeable about disclosure requirements under the federal securities laws.
- An independent auditor with experience in the accounting rules particular to your industry and to your company's business model.

In addition to these basic features, which are essential to protecting the company and its officers from allegations of securities fraud, you need to take steps to protect yourself from allegations of securities fraud. CEOs are often in the sights of government enforcement teams during securities fraud investigations, and your knowledge about or role in any challenged statements will receive significant scrutiny.

Here are ten things you can do to protect yourself and reduce your exposure to charges of securities fraud:

1. Have your public speeches and presentations reviewed for accuracy by your CFO and counsel and other knowledgeable employees who can help flag inaccuracies.
2. Develop a system for reviewing the important details of your annual SEC filings before signing the SOX certifications that accompany those filings. Make sure you understand each paragraph of the SOX certificate and what has been done to ensure its accuracy.
3. Use a prepared script for quarterly conference calls, and develop written talking points for anticipated questions from call participants.
4. Implement a 10b-5-1 trading plan for your anticipated transactions in the company's stock and options.
5. Develop a procedure for complying with Reg. FD, which prohibits selective disclosure of material information to analysts or large investors.
6. When preparing to make public remarks, consider the most important points and ensure that you understand the support for why those points are accurate and not misleading.
7. When inevitable problems arise, of whatever nature, obtain advice from counsel about the appropriate public disclosures that are required.
8. Develop an understanding of the most critical accounting policies for your company, and avoid pushing the envelope and being overly aggressive in interpreting the applicable accounting rules for those critical areas.
9. Meet at least once each year with your outside auditors, and encourage them to bring important issues to your attention.
10. Promote a culture of compliance with the applicable legal rules and regulations that permeates your company, and encourage your employees and top managers to maintain high ethical standards. The tone at the top can help keep you and your company out of trouble.

PART IV. FOREIGN CORRUPT PRACTICES ACT

A. WHAT IS AT STAKE

Congress passed the Foreign Corrupt Practices Act ("FCPA") in 1977 in response to reports that numerous U.S. businesses were making large payments to foreign officials to get business abroad. In recent years, there has been an unprecedented surge of anti-corruption enforcement activity by the SEC and the DOJ.

Violations of the FCPA committed by your company can result in civil or criminal enforcement. As a CEO, you may be held personally liable for FCPA violations. Penalties for violations include monetary fines as well as prison sentences.

This section provides an overview of what a CEO needs to know about the FCPA to manage these liability risks.

Case Study: In May 2011, a jury returned guilty verdicts for a small, privately held corporation (and two top executives and a third-party intermediary), convicting the company of six FCPA counts for securing business contracts by passing a 30% commission to foreign officials in exchange for the officials steering contracts to the company. The convictions were later thrown out on grounds of prosecutorial misconduct, but this case foreshadows the type of rigorous enforcement activity that should be expected in the future.

B. LEGAL BRIEFING

Key Provisions. There are three key provisions of the FCPA:

- Anti-Bribery: It is illegal to give, offer, or promise money or anything of value to a foreign government official or foreign political party with the intent to obtain or retain business.
- Books and Records: Businesses must make and keep accurate books, records, and accounts.
- Internal Controls: Businesses must develop and maintain reasonable internal accounting controls to prevent and detect FCPA violations.

Corporate Liability. FCPA violations may cost a business millions of dollars in fines, but the collateral consequences of these violations may be even more costly in the long run.

Consider these additional expenses associated with FCPA violations:

- Even though the FCPA provides no private right of action, collateral civil suits are increasing in number and scope.
- Investigations may cost millions of dollars and span multiple years.

- Monitorships imposed by settlement agreements can cost additional millions of dollars and last for many years.
- Ratings agencies may lower credit ratings for financially strained companies that have FCPA violations.

Individual Liability. Even after U.S. regulators enter into a negotiated settlement with a business, individual employees are not free from FCPA liability. Regulators are increasingly likely to bring additional enforcement actions against individuals, including CEOs, sometimes years after a settlement has been reached.

Individual accountability under the FCPA requires the necessary intent. An individual must intend to do something the law forbids, *but:*

- The individual does not need to be aware of the specific law and rule that is being violated; and
- Even if the offer to pay a bribe is rejected or payment is never made, a violation may still occur.

Penalties. An entity or individual may be prosecuted under the FCPA for criminal violations, civil violations, or both. The following chart lists maximum penalties for common charges related to entity and individual FCPA violations:

VIOLATION	PENALTY
Criminal Penalties	
Anti-Bribery Violations	• *Entities:* Up to $2,000,000 per violation (or more under alternative fine rules) • *Individuals:* Up to $100,000 per violation and imprisonment for up to 5 years
Books-and-Records Violations	• *Entities:* Up to $25,000,000 per violation (or more under alternative fine rules) • *Individuals:* Up to $5,000,000 and imprisonment for up to 20 years
Conspiracy to violate FCPA	• *Individuals:* Up to $250,000 or twice the value gained or lost and imprisonment for up to 5 years
Wire fraud	• *Individuals:* Up to $250,000 or twice the value gained or lost and imprisonment for up to 5 years
Conspiracy to commit money laundering	• *Individuals:* Up to $500,000 or twice the value gained or lost and imprisonment for up to 20 years
Civil Penalties	
Anti-Bribery Violations	• *Entities:* Up to $10,000 per violation; SEC may seek an injunction and/or an additional fine of up to $500,000 on the gain obtained as a result of the violation • *Individuals:* Up to $10,000 per violation
FCPA-Related Civil Liability (under derivative lawsuits, securities fraud actions, tort and contract law claims, employment lawsuits, and private actions under RICO)	• *Entities and Individuals:* Varies depending on claim

Select Defenses to FCPA Liability

The following are narrow exceptions and defenses to FCPA liability:

- *Facilitation Payments:* There is a *narrow* exception for payments used to secure the performance of a routine, non-discretionary government action that is essentially ministerial in nature.
- *Lawful Payments under Written Laws:* That the law of the foreign country expressly requires or permits the recipient to be influenced by the offer or gift can be raised as an affirmative defense. However, this defense is not available if the laws of the foreign country are silent on the matter.
- *Reasonable and Bona Fide Expenditures:* Payment in question is a reasonable and bona fide expenditure, such as travel and lodging costs or expenses related to the promotion of services or the execution of a contract. However, whether an expense will be considered legal depends on the facts surrounding the payment.

C. FCPA RISK ASSESSMENT

Are you and your company aware of the activities that may implicate the FCPA? If you answer "yes" to any of the following questions, your company may be at risk for FCPA violations:

- Do you conduct business or have operations outside the United States?
- Do you interact with employees of foreign government-owned businesses?
- Do you use third-party agents in foreign countries?
- Are you considering acquiring a company that conducts business or has operations outside the United States?
- Does your company have foreign subsidiaries?
- Are you a minority shareholder in a joint venture?

Negotiating the requirements of the FCPA can be challenging, particularly when businesses engage with local agents in foreign countries. The good news is that being mindful of the risks associated with the FCPA, and creating and enforcing effective compliance protocols, will help you manage these risks.

Below are some of the key risks that the CEO should keep in mind when doing business in foreign countries:

Risk #1: Willful Blindness

Even if an individual does not personally violate the FCPA, he may be accountable for the violation if he "knows" about the misconduct. A person knows about misconduct if he:

- Is aware of the misconduct,
- Is substantially certain that the misconduct will occur, or
- Consciously disregards a high probability that the misconduct will occur.

A person cannot, however, avoid liability by being "willfully blind," meaning he cannot deliberately avoid confirming his suspicions of misconduct. On the other hand, a person does not "know" about misconduct if he:

- Actually believes the transaction is legal, or
- Fails to learn the facts because of negligence.

Case Study: Recently, the co-founder of a major corporation was convicted of conspiring to violate the FCPA and the Travel Act. The defendant made an investment in a business venture that paid millions of dollars in bribes to foreign officials. In deciding the outcome of the case, the jury was given an "ostrich instruction": knowledge may be established when a juror can conclude a person deliberately avoids confirming suspicions that a business partner or associate may be paying bribes to foreign officials.

Risk #2: Third-Party Agents

The FCPA prohibits businesses from making payments to third parties if they know that some of the money will be used inappropriately. Third parties can include joint venture partners, suppliers, contractors, and agents. This can prove especially challenging for companies that do business in foreign countries through local agents. To mitigate this risk, it is a good idea to include anti-corruption provisions in contracts with third parties.

Risk #3: Government-Owned Businesses

The FCPA interpretation of "foreign officials" is very broad. It includes government-owned or controlled businesses and enterprises, whether fully or partly government-owned. This means that companies must be very cautious when interacting with any employee of a government-owned or controlled business, because the employee may be considered a "foreign official." The distinction is particularly important for companies conducting business in countries with many government-owned businesses, such as China. Whether or not the employee will actually be considered a foreign official is determined on a case-by-case basis, and depends on multiple factors.

Risk #4: Foreign Subsidiaries

A U.S. parent company may face liability for actions of its foreign subsidiary if the parent company:

- Authorized, directed, or controlled the activity,
- Knew about the activity, or
- Consciously disregarded the substantial risk of the activity.

Therefore, consider providing extensive compliance procedures for your foreign subsidiaries.

Risk #5: Successor Liability

In a merger or acquisition, an acquiring company can inherit FCPA violations of the target company. The key issues to be aware of are:

- *Pre-acquisition misconduct:* failure to perform proper due diligence before acquiring a new company; and
- *Post-acquisition misconduct:* continued violations caused by deficiencies in the acquired company's compliance and control procedures.

Thorough pre-acquisition due diligence and post-acquisition compliance integration can mitigate this risk. If potential violations are identified during your due diligence, consider self-reporting them prior to closing the deal.

Risk #6: Joint Ventures

The FCPA recognizes that minority shareholders may not have full control over company procedures. However, a minority shareholder has an affirmative obligation to try in good faith to implement procedures consistent with FCPA accounting provisions. Therefore, if your company holds a minor stake in a joint venture, demonstrate good faith efforts to comply with the law. Adopt a minority joint venture policy that establishes guidelines for the company to evaluate joint venture relationships before entering into them and throughout their duration.

Risk #7: Global Anti-Corruption Enforcement

For many years, businesses could feel confident that as long as they complied with the FCPA, their actions also complied with non-U.S. bribery and corruption laws. As many countries throughout the world increase their enforcement efforts, however, simply complying with the FCPA provisions may not be enough. Instead, businesses must ensure that they do not run afoul of these new—and potentially more rigorous—global rules and requirements. For instance, the UK Bribery Act, passed in 2010, contains strict regulations and applies regardless of where the alleged bribery occurs.

D. CEO ACTION PLAN

When facing a government investigation of potential FCPA violations, your goal is to convince the prosecutor not to prosecute the company. The DOJ Fraud Section Chief explained that corporate declinations are generally based on three factors:

- The adequacy of the company's compliance program;
- The thoroughness of the company's cooperation with the DOJ; and
- Whether the company self-disclosed the conduct to the DOJ.

Compliance Programs

Good corporate governance pays off every time. Comprehensive and well-written policies and procedures are key to managing many risks, including those associated with FCPA violations. In addition to effective policies governing corporate basics such as accounting procedures and internal controls, it may be appropriate for companies to establish targeted policies and procedures to govern interactions and relationships with foreign officials. These should be distributed to all affected employees and third parties. Further, employees should receive anti-corruption and local law compliance training. Strong compliance programs may also be a defense to civil suits.

Monitoring

Excellent compliance programs are of little use if they are not properly implemented. Companies should perform risk-based continuing monitoring of compliance programs to determine their effectiveness, and adjust the programs as necessary. A hotline or other reporting process helps to identify potential concerns and stop potential violations before they occur. Whistleblower policies should be designed to protect those who do report concerns. In addition, recurring operational audits may be helpful to identify the effectiveness of established policies and procedures.

Consider Voluntary Self-Disclosure

If you become aware of potential misconduct, it may be in the company's best interest to disclose such information. This may be a complex decision and should be made in consultation with your legal counsel, but cooperation with the government has been cited by the Department of Justice as a factor in determining whether or not to proceed with charges.

PART V. DATA PRIVACY

A. WHAT IS AT STAKE

CEOs should be aware of the existence of various regulations and restrictions on data disclosure, internationally and domestically, that can lead to serious issues for companies involved in litigation and government or internal investigations. Additionally, a company's collection or use of customer data in the ordinary course of business may also lead to potential liability and regulatory scrutiny which, in a number of well publicized international cases, has led to criminal action being taken against company executives.

Consider the following hypothetical: You've just been informed that a salesperson in your company's subsidiary in China may have used a consultant to give a kickback to a Chinese government official in order to secure a major contract. The salesperson's supervisors are located in Hong Kong and France. The U.S. DOJ has been tipped off and is preparing to investigate, and there is the potential for follow-on civil lawsuits. You need to conduct an internal investigation, including obtaining e-mails and records of the salesperson, the supervisors, and the third-party consultant, as well as records concerning the Chinese official.

In this situation, Chinese, French, and European Union regulations may prevent the cross-border transfer or processing of your employees' electronic and non-electronic records. You may be limited in your ability to discipline your employees for misconduct in light of local employment laws. And you may not be able to obtain or transfer Chinese government-related data due to national security concerns. Your managers in China and France may also face local penal sanctions if they cooperate with the investigation.

Further, once your investigation is complete, you may not be able to disclose what you have learned to the U.S. DOJ or comply with U.S.-based civil discovery orders without violating the privacy laws of other jurisdictions. Finally, the laws of different jurisdictions may be incompatible, forcing you to choose between complying with a U.S. subpoena to turn over an employee's data, or with another jurisdiction's law prohibiting transfer of that data without the employee's consent.

Even if local privacy requirements do not prevent the investigation or discovery from taking place, they can substantially increase the costs and time involved in carrying out investigations. While local legal compliance is important, there are relatively few legal precedents in this area, and it is important that companies consider local legal risks in the context of how such laws are enforced. A pragmatic, risk-based approach is generally appropriate in these situations.

While CEOs are not generally expected to know and understand all the applicable laws, they should have an awareness of when legal advice is needed. CEOs who either personally inadvertently violate, or instruct employees to inadvertently violate, foreign laws may be subject to criminal liability, including fines and imprisonment in non-U.S. jurisdictions.

Although there is no coherent federal statutory scheme regulating the use or disclosure of personal data in the U.S., government agencies and private litigants frequently attempt to address data privacy concerns through the use of computer crime laws or under "breach of representation" theories. In addition, certain statutes impose specific requirements on companies engaged in the collection or use of data involving specific groups (such as children) or impose restrictions upon data practices of certain industries (such as healthcare).

Nonetheless, CEOs should be aware of the increasing focus by the government and private litigants on privacy issues in the U.S., and companies in the U.S. have increasingly been subject to costly class action lawsuits and regulatory scrutiny in privacy-related matters.

B. LEGAL BRIEFING

Data privacy restrictions, especially in foreign jurisdictions, may impact a company's efforts to act swiftly in the following matters:

- Civil suits
- Regulatory actions
- Criminal investigations
- Internal investigations
- Employee discipline matters

For example, a company involved in litigation or an internal investigation may not be able to gather or produce relevant e-mails from overseas, or may not be able to interview an employee with key information. If an employee in a foreign jurisdiction refuses to cooperate with a company's investigation, the company may not be able to lawfully terminate employment unless the company has complied with local employment procedures, which may slow the investigation.

Likewise, U.S. and international privacy laws can affect a company's ability to conduct business or make use of customer data. These laws, or consumer litigation challenging a company's privacy practices, can have a significant impact on a company's ability to outsource or offshore business processes, sell or commercialize information, market to consumers, and offer innovative new products and services. For example, Google entered into an $8.5 million settlement in a class-action lawsuit that alleged that Google Buzz violated users' privacy.[1]

There are various types of regulations and statutes that restrict the access, use, or transfer of data, including employee and customer data. There is sometimes confusion over terminology, and different laws often provide overlapping protections. Nonetheless, these laws broadly fall into the following categories:

1 Amir Efrati, Google Settles Privacy Lawsuit for $8.5 Million, *Wall Street Journal* (Sept. 3, 2010).

- *Data Transfer Regulations:* Regulations or statutes, often included within larger data protection laws, that require companies to follow certain procedures and provide notifications to employees before transferring data to other parties or across jurisdictions.
- *Blocking Statutes:* statutes designed specifically to preclude compliance with foreign discovery requests which shortcut international treaty obligations.
- *Data Protection Laws:* Laws of general application that seek to balance the rights of data subjects against the rights of companies that control their data.
- *Monitoring Laws:* Laws restricting the monitoring of communications that may give employees a right of privacy in relation to their work communications.
- *Data Mining Laws:* Laws that regulate the collection and use of large quantities of consumer data.
- *Data Breach Laws:* Laws that require companies to notify individuals when personal data held by those companies are compromised.

There are also specific laws that may apply in particular sectors, such as banking, financial services, healthcare, and defense. Other laws, such as employment laws, may also affect cross-border investigations. For example, in Germany the consent or notification of works councils (the local firm-level employee representation bodies) may be required before employers are permitted to start internal investigations. This particularly concerns reviewing employee e-mails or conducting interviews.

Data Transfer Regulations

Data transfer regulations address the following types of materials:

- Individual or personal data
- State secrets
- Trade secrets
- E-mail and other electronic communications
- Individual or collective employment rights

Data transfer regulations may require companies to follow certain procedures and provide notifications to employees and other data subjects before transferring data. Further, some jurisdictions have blocking statutes (discussed further below), expressly prohibiting certain types of data to be transferred for various enumerated purposes. For example, transferring data for internal investigations may be permitted under a blocking statute, while providing data to a government entity or civil litigant may not.

Blocking Statutes

Blocking statutes are statutes designed specifically to preclude compliance with foreign discovery requests in certain areas, and instead require U.S. litigants and regulators to avail themselves of international treaties providing for mutual administrative and legal assistance. These blocking statutes are designed to protect the territorial sovereignty of the jurisdiction concerned over what they perceive to be the unwarranted territorial application of foreign and particularly U.S. laws.

These statutes:

- Vary by jurisdiction,
- Are primarily designed to block broad-based, U.S.-style discovery, and
- Usually carry the potential for criminal and civil liability.

Sample Blocking Statutes:

- *Europe:* It is illegal in several countries, including Switzerland and France, to follow certain foreign procedural rules, including the gathering of documents and deposition of witnesses for foreign litigation or investigations outside of the Hague Evidence Convention, an international treaty governing cross-border evidence transfer.

Case Study: A violation of France's blocking statute resulted in personal criminal liability for a French attorney in 2007, after a U.S. court ordered a French bank to comply with a discovery request to produce documents from France, despite a French law prohibiting the data transfer. Subsequent to the French bank's compliance with the discovery request, a French attorney who facilitated the transfer of the documents was convicted on criminal charges and ordered to pay a €10,000 fine. The conviction was later upheld by the French Supreme Court.[2]

- *China:* China's State Secrecy Law criminalizes disclosure of any information deemed to be a state secret.

Data Protection Laws

The right to privacy of personal data is accorded significantly greater weight in many jurisdictions outside the U.S. Many countries have enacted general data protection laws that have general application to all or most data processing operations. As of July 30, 2011, there were 76 foreign countries with general privacy laws based upon the model set by the Organisation for Economic Co-operation and Development ("OECD").

These laws differ significantly, but the OECD model includes the following guidelines for the protection of privacy:

2 See *In re Advocat Christopher X, Cour de Cassation*, Chambre Criminelle, Paris, Dec. 12, 2007, No. 07-83228 (the French criminal case); *Strauss v. Credit Lyonnais S.A.*, 242 F.R.D. 199 (E.D.N.Y. 2007) (the United States case from which the discovery order originated).

- *Collection:* Data should only be collected by lawful means, where appropriate, with the knowledge or consent of the data subject.
- *Data Quality:* Data must be relevant, accurate, complete, and kept up-to-date.
- *Specified Purpose:* Data should be collected for a specific purpose and not used later for other incompatible purposes.
- *Use Limitation Principle:* Personal data should not be disclosed to others without consent of the data subject or the authority of law.
- *Information Security:* Data should be protected by reasonable security safeguards against loss or unauthorized access, use, or disclosure.
- *Notice:* The entity which controls the data should disclose and be open about its policies and practices.
- *Access:* An individual should have a right to access his personal data, to challenge data relating to him, and if successful to have the data erased, rectified, completed, or amended.
- *Free Flow of Data:* Data should flow freely to all states that follow the guidelines.

Sample Data Protection Laws:

- *The European Union (EU):* The European Union Data Protection Directive (the "Directive") is perhaps the most well-known general privacy law and has been adopted by each EU member state. However, there are significant differences between member states in the ways that the legislation is implemented and enforced, so it is rarely possible to take a single approach to the entire EU. The Directive was broadly based on OECD guidelines for the protection of privacy. Under the Directive:
  - » Personal data is broadly defined to include "any information relating to an identified or identifiable natural person" which potentially includes non- traditional identifiers such as usernames and details of employees' involvement in work and non-work related matters.
  - » All "processing" of personal data is regulated, whether in the form of the collection, storage, copying, review, storage, or disclosure of data. In contrast to the U.S., under the Directive, processing does not need to be automated and would include reviewing an employee's e-mails or using certain manual filing systems.
  - » More onerous protections apply to the processing of "sensitive personal data" (such as personal data relating to sex life, race, political affiliation, union membership, and health), which often requires explicit consent.
  - » The local entity that controls the personal data is prohibited from transferring it outside the European Union or other countries deemed to have "adequate"

protection. Generally, the United States is not deemed to have adequate protection, but there are exceptions to this rule.

- *China:* China has its own unique data protection laws that criminalize the disclosure or cross-border transfer of state secrets and archives.
  - » "State secrets" are broadly defined as "matters that have a vital bearing on state security and national interests and, as determined according to statutory procedures, are known by people within a certain scope for a given period of time."
  - » Computer information systems that store or handle state secrets must be protected by security measures, and actions that compromise the security of electronic state secrets are prohibited.
  - » China's state secrets law has been invoked against foreign nationals, as well as Chinese citizens providing state secrets to foreigners. For example, in 2010, U.S. citizen Xue Feng was sentenced to eight years' imprisonment for allegedly obtaining and selling a database showing the locations and conditions of many oil and gas wells in China. In this instance, the database was retroactively classified as a state secret, demonstrating the difficulty of compliance with Chinese data transfer laws.
  - » Violations of the state secrets law carry administrative liability, as well as criminal penalties (imprisonment, criminal detention, public surveillance, deprivation of political rights, forfeiture, and/or death).
  - » China also prohibits the cross-border transportation of archives or duplicates. "Archives" are broadly defined as "historical records . . . whose preservation is of value to the State and society and which have been or are being formed by State organs, public organizations and individuals in their [various] activities." The law may cover documents such as corporate formation documents, contracts, financial and accounting records, and personnel files.
  - » Customs officials may legally confiscate such materials and fines and criminal liability are possible.
- *India:* Under India's brand new data privacy laws, sensitive data or information can only be disclosed by a corporate entity to a third party if prior consent has been obtained from the data provider, unless otherwise provided for by contract or by law. However, the Indian government released a press note in August 2011 clarifying that foreign companies are excluded from the ambit of the obligations imposed by the new data privacy rules.
- *Argentina:* Argentina's federal Data Protection Act states that the treatment of personal data is unlawful unless individuals have given their express consent in writing or similar means. Implied consent is not sufficient.

- *Brazil:* A data protection bill in Brazil allows the right to protection of personal data to be invoked, either individually or collectively, and mandates that each private entity nominate a Chief Privacy Officer.
- *U.S.:*
  - » There is no federal law that governs data protection broadly. Instead, it is regulated in specific contexts (such as privacy for children) or in specific industries (such as healthcare). However, several states have passed laws that impose disclosure requirements or other obligations on companies that collect personal information from consumers.
  - » In the various statutes and regulations, protected personal data is generally construed more narrowly as only encompassing highly sensitive or personally identifying information (e.g., medical and banking information, SSNs, e-mail addresses). The Federal Trade Commission (FTC) has recently proposed regulations revising the scope of information encompassed by the Children's Online Privacy and Protection Act to include "persistent identifiers" and other anonymous information that has not traditionally been considered personal data in the U.S.
  - » Section 5 of the FTC Act prohibits "unfair" or "deceptive" trade practices. This provision provides broad consumer protection, but is not specific to privacy. The FTC has used its Section 5 authority, however, to pursue claims targeting a number of wide-ranging data privacy concerns and practices—particularly in the online and mobile environment.

Monitoring Laws

Monitoring laws govern what types of information data controllers, such as employers, may monitor, collect, and analyze, and what types of disclosure or consent may be required. For example:

- *China:* Chinese laws are vague regarding the right of employers to access and/or monitor their employees' data. Chinese government officials recommend that written consent be obtained from an employee (e.g., before accessing or monitoring the employee's e-mails), although this is not explicitly required under the law.
- *EU:* Member states are required to ensure confidentiality of communications through publicly available communications servers. This regulates the extent to which employers can monitor or otherwise intercept employee communications without user consent.

Data Mining Laws

Data mining laws are laws protecting consumers' privacy that regulate the analyses of large quantities of data. These laws are in response to an overall greater ability to compile more data with faster transmission speeds and more powerful computing, as well as to more complex online ecosystems.

Sample Data Mining Statutes:

- *EU:* These data mining practices would be regulated by the general data protection laws and would at the very least require fair notice and the balancing of the rights of data subjects against the interests of the data miners. The EU is also in the process of enacting legislation that will require users to opt in to the use of "cookies" and similar devices which track their online behavior.

Data Breach Laws

Many countries have laws that require companies to notify individuals when personal data held by those companies is compromised by a security breach. Again, the types of data covered and the form of the required notification vary by jurisdiction.

Sample Data Breach Statutes:

- *Germany:* Germany requires immediate notification of breaches that would lead to "significant harm" to individuals.
- *Mexico:* Under Mexico's new data protection legal framework, the Data Protection Authority (the "DPA") will not need to wait for an individual to complain before launching an investigation—there is a "reasonable doubt" trigger for investigations.
- *U.S. Federal Government:* The SEC has issued disclosure guidance regarding cybersecurity risks and cyber incidents, and identified seven areas in companies' SEC filings that may require a statement about cybersecurity risks or incidents:
  - » Risk Factors
  - » Management's Discussion and Analysis
  - » Descriptions of Business
  - » Legal Proceedings
  - » Financial Statement Disclosures
  - » Disclosure Controls and Procedures
  - » Form 8-K
- *U.S.:* More than 30 U.S. states also regulate data breach and data privacy domestically. Some states require an additional notification to a state regulator or the state attorney general. There are also substantive data security protections for certain types of sensitive data, such as banking records or medical information, under state law.

C. CEO ACTION PLAN

CEOs should work with counsel to create and maintain internal protocols to address data privacy issues when they arise—and to ensure that their companies' day-to-day operations do not pose data privacy compliance concerns. Companies may also need to establish internal and external privacy policies regarding the use and protection of customer data.

U.S. law firms can assist in drafting policies, training employees, and identifying when local counsel should be engaged. However, it is often advisable to retain local counsel on a case-by-case basis as the need arises to ensure that no inadvertent violations of laws occur in a specific matter or investigation. In addition, in many jurisdictions, only locally qualified counsel are permitted to provide legal advice on local law.

Immediate Action Plan

- Conduct a baseline assessment to understand what data the company collects, analyzes, processes, retains, what purposes it uses the data for, and the third parties to which it is disclosed. The assessment should also consider where that data is located and any cross-border data flows. Compiling a "data map" can be extremely useful.
- Carry out a risk assessment and a compliance audit.
- Establish policies to prevent the inadvertent receipt, use, and transmission of state secret, trade secret, and personal information materials.
- Establish employment and privacy policies in the relevant jurisdictions that describe the company's procedures for collecting, analyzing, processing, transferring, and storing personal information, and provide contact information to handle specific complaints and inquiries.
- Establish internal data security protocols in coordination with IT vendors and, where relevant, customers.
- Establish a data breach response plan with designated responsibilities.
- Establish a data retention policy for paper and electronic records.
- Allocate responsibility for information governance. Larger companies, those in regulated industries, or those processing large volumes of consumer data should consider appointing specialist privacy professionals.

Ongoing and Unscheduled Action Plan

- In jurisdictions with broad or ambiguous statutes, such as China, use extra caution when dealing with government entities, state-owned enterprises, overseas listed companies, or other entities that may draw heightened scrutiny.

- Provide training to U.S. employees and litigants on state secrets, trade secrets, personal data, their identification, and liability associated with their unauthorized possession, use, and transmission.

Annual Action Plan

- Review data security, privacy policy, incident response plan, employee training, and data assessment to ensure that changes in the business or in the regulatory environment are addressed.

D. BOTTOM LINE

There are myriad laws addressing data privacy, data transfer, and data security issues that can arise in or give rise to litigation, government actions, and investigations, and they vary widely by jurisdiction. Accordingly, companies should develop a sensitivity to potential data privacy issues in order to mitigate the risk of an inadvertent violation of a local law and, if necessary, engage qualified counsel to provide a specific analysis of any particular situation and develop a commercially pragmatic response.

PART VI. ADDITIONAL RESOURCES

A. GENERAL WHITE COLLAR CRIMINAL DEFENSE RESOURCES

- DOJ, *Principles of Federal Prosecution of Business Organizations*, USAM §§ 9-28.000 *et seq.*, available at: http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/28mcrm.htm
- U.S. Sentencing Commission, *Sentencing of Organizations*, in Federal Sentencing Guidelines Manual chap. 8, available at: http://www.ussc.gov/Guidelines/Organizational_Guidelines/guidelines_chapter_8.htm
- Gibson Dunn Client Alert, *2011 Year-End Update on Corporate Deferred Prosecution and Non-Prosecution Agreements,* available at: http://www.gibsondunn.com/publications/Pages/2011YearEndUpdate-CorporateDeferredProsecution-NonProsecutionAgreements.aspx. An overview of FCPA developments in 2011. Updates are published semi-annually, and can be found at: http://www.gibsondunn.com/Search/Pages/PublicationsSearch.aspx?k=('Publication Practice':'White Collar Defense and Investigations')
- White Collar Crime Prof Blog, available at: http://lawprofessors.typepad.com/whitecollarcrime_blog. A blog providing news and commentary related to white collar criminal law.

B. SECURITIES FRAUD RESOURCES

- The text of federal securities statutes and regulations are available at: http://sec.gov/about/laws.shtml
- SEC Litigation releases concerning federal civil actions brought by the SEC are available at: http://sec.gov/litigation/litreleases.shtml
- Notices and orders concerning SEC administrative proceedings are available at: http://sec.gov/litigation/admin.shtml
- Gibson Dunn Client Alert, *2011 Year-End Securities Enforcement Update, available at:* http://www.gibsondunn.com/publications/Pages/2011YearEndSecuritiesEnforcementUpdate.aspx An overview of securities enforcement developments in 2011. Updates are published semi-annually, and can be found at: http://www.gibsondunn.com/Search/Pages/PublicationsSearch.aspx?k=('Publication Practice':'Securities Enforcement')
- Securities Law Prof Blog, available at: http://lawprofessors.typepad.com/securities/. A blog providing news and commentary on securities law developments.

C. FOREIGN CORRUPT PRACTICES ACT RESOURCES

- Foreign Corrupt Practices Act, 15 U.S.C. § 78dd-1 et seq., 18 U.S.C. § 371, available at: http://www.justice.gov/criminal/fraud/fcpa/statutes/regulations.html
- UK Bribery Act, available at: http://www.legislation.gov.uk/ukpga/2010/23/contents
- A complete list of FCPA and related enforcement actions is available at: http://www.justice.gov/criminal/fraud/fcpa/cases/a.html
- Gibson Dunn Client Alert, *2011 Year-End FCPA Update, available at:* http://www.gibsondunn.com/publications/Pages/2011YearEndFCPAUpdate.aspx. An overview of FCPA developments in 2011. Updates are published semi-annually, and can be found at: http://www.gibsondunn.com/Search/Pages/PublicationsSearch.aspx?k=('Publication Practice':'White Collar Defense and Investigations')

D. DATA PRIVACY RESOURCES

- European Commission, *Protection of Personal Data, available at:* http://ec.europa.eu/justice/data-protection/index_en.htm. The European Commission's website with numerous resources on the European Union's data protection laws, regulations, and policies.
- European Commission, *Data Protection Guide, available at:* http://ec.europa.eu/justice/policies/privacy/guide/index_en.htm . A listing of country-specific data protection guides in local languages aimed at individual consumers.
- National Conference of State Legislatures, *State Security Breach Notification Laws, available at:* http://www.ncsl.org/default.aspx?tabid=13489. A compilation of U.S. state laws addressing security breach notification requirements.
- Gibson Dunn Client Alert, *Data Privacy Rules Enacted in India, available at:* http://www.gibsondunn.com/publications/Pages/DataPrivacyRulesEnactedinIndia.aspx. An article highlighting and analyzing the Data Privacy Rules enacted by the Indian government in April 2011.
- Gareth T. Evans and Farrah Pepper, Digital Discovery & E-Evidence, *Court Holds U.S. Discovery Rules Trump French Law and Hague Convention (December 1, 2009).* An article addressing the controversy where a U.S. court issued a discovery order to a French bank relating to documents in France. The production of those documents led to the prosecution of a French attorney who complied with the discovery order for violating French data transfer laws.
- Catherine Brewer and Gareth T. Evans, EuroWatch, *French Data Protection Authority Announces Increased Inspections for Compliance with French and European Union Data Privacy Requirement (June 15, 2011).* An article describing the French Data Protection Authority's announcement that it would seek to more aggressively enforce French and European Union data protection laws and regulations.