
## Tuesday, October 20
## 9:00 am–10:30 am

# 105 Conducting Corporate Investigations- The Use of Lawful and Ethical Strategies

**Daniel Karson**
*Senior Counsel*
Kroll Associates, Inc.

**John Lewis**
*Senior Managing Counsel- Litigation*
The Coca-Cola Company

**Ralph Martin II**
*Partner*
Bingham McCutcheoun, LLP

**Marcia Narine**
*VP, Global Compliance & Business Standards/ Deputy GC*
Ryder System, Inc.

# Faculty Biographies

**Daniel Karson**

Daniel Karson serves as senior counsel for Kroll Associates in New York. His responsibilities include legal and risk assessment for Kroll and counseling clients on risk strategies. Mr. Karson has experience directing investigations of business crimes and regulatory violations. His notable cases include major investigations of internal corporate frauds, violations of the Foreign Corrupt Practices Act, Internet crimes, and complex litigation.

Prior to joining Kroll, Mr. Karson was general counsel and assistant commissioner of the New York City Department of Investigation. He was the first director of the city's inspector general program and directed investigations and determined policy for the internal investigative offices of 24 mayoral agencies. Previously he worked as an assistant district attorney for Bronx County, New York, where he served as chief of narcotics investigations.

Mr. Karson is a member of ACC and is a member of the board of directors of ACC's Greater New York Chapter. He is a frequent speaker at ACC and other professional association meetings, most often on the subject of conducting corporate investigations and compliance.

He graduated from Ithaca College and New York University Law School.

**John Lewis**

John Lewis Jr. is senior managing litigation counsel for The Coca-Cola Company in its global legal center in Atlanta. In his current role, Mr. Lewis manages the attorneys and staff responsible for litigation and disputes throughout the over 200 countries where the company does business. His group partners with outside counsel to advise internal clients in a variety of areas including commercial disputes, securities litigation, shareholder derivative actions, governmental/internal investigations, intellectual property, international disputes, arbitration, and employment disputes. He also leads Coca-Cola legal's global diversity initiative and is actively designing an integrated diversity strategic plan for the legal division. In addition, Coke's senior vice president and general counsel, Geoff Kelly, appointed Mr. Lewis to serve as the division's representative on the Company-wide nine member corporate diversity advisory council (DAC).

He joined Coca-Cola after several years in private practice as a commercial litigator.

Mr. Lewis serves as vice-chair of the board of The Coca-Cola Company Family Federal Credit Union and chair of the City of Atlanta Board of Ethics.

Mr. Lewis is an honors graduate of Morehouse College and holds a JD from The George Washington University National Law Center.

**Ralph Martin II**

Ralph Martin is the managing partner of Bingham's Boston office as well as managing principal of Bingham Consulting Group. Bingham Consulting advises clients who are challenged by the legal, public policy, and other complexities of multi-state investigations by Attorneys General. He practices in the areas of corporate investigations, white collar defense, and general civil litigation.

Mr. Martin is the former Suffolk County district attorney, having served as the elected prosecutor for Boston, Chelsea, Revere, and Winthrop. He has extensive experience as a trial lawyer and as state and federal prosecutor.

Mr. Martin is co-chair of the firm's national diversity committee. Mr. Martin is a trustee of Children's Hospital, a director of Blue Cross Blue Shield of Massachusetts, and a former chairman of the Greater Boston Chamber of Commerce, the region's leading business advocacy group. He is a member of the advisory committee to former U.S. Senator Ted Kennedy on judicial and federal appointments and former chairman of the judicial nominating committee.

Mr. Martin received a BA from Brandeis University and a JC from Northeastern University School of Law.

**Marcia Narine**

Marcia Narine is vice president and deputy general counsel, as well the vice president, global compliance and business standards and chief privacy officer of Ryder System, Inc. in Miami. She oversees the company's global compliance, business ethics, privacy, government relations, environmental compliance, enterprise risk management, and labor and employment legal programs, as well as Ryder Fuel compliance services, which helps companies improve operating efficiencies and minimize environmental impacts.

Before joining Ryder, Ms. Narine was an associate with Morgan, Lewis and Bockius' labor and employment practice in Miami. She worked as a commercial litigator with Cleary, Gottlieb, Steen and Hamilton in New York, and was a law clerk to former Justice Marie Garibaldi of the Supreme Court of New Jersey.

She is a member of Leadership Florida- Class XXVII, the Caribbean Bar Association, the Gwen S. Cherry Black Women Lawyer's Association, and the Wilkie D. Ferguson Bar Association. She is also on the editorial board of the Society of Corporate Compliance & Ethics magazine; a member of the Ethics and Compliance Officer Association; and a court-appointed guardian ad litem for abused and neglected children. She has served on the advisory committee of the National Association of Minority and Women Owned Law Firms, on the advisory board of Teach For America (Miami region), and as a Cub Scout

 

Pack Chairperson. She was named in the 2009 Women Worth Watching edition of the Profiles in *Women Diversity Journal*.

Ms. Narine earned a BA from Columbia University and graduated cum laude from Harvard Law School.

 

# Association of Corporate Counsel – Annual Meeting
# Session 105
# Conducting Corporate Investigations — The Use of Lawful and Ethical Strategies

## Outline*

Daniel E. Karson · Senior Counsel - Kroll Associates, Inc.
212-833·3266 · dkarson@kroll.com- www.kroll.com

## I. What Kind of Cases Call for an Investigation?

- Internal investigations: Contract/Purchasing Fraud. Examples:
  - Kickbacks paid by vendors
  - An employee has an undisclosed ownership interest in a vendor
  - Fictitious vendor scheme – (An employee sets up a company; the employee bills the corporation for fictitious services and causes payments to be made to the fictitious company.)

- Foreign Corrupt Practices Act
  - Bribes paid to government officials by employees
  - Bribes paid to government officials through corporate agents or representatives

- Theft of intellectual property/trade secrets
  - Stealing private data
  - Selling private data to competitors
  - Laying the groundwork to quit and set up a competing firm, using company IP

- Internet Torts and Crimes
  - Defamation of company name, corporate officers, etc. through anonymous emails, blogs, bulletin boards, chat rooms and social networking sites
  - Extortionate threats to do harm and damage
  - Disclosure of confidential information
  - Hacking into mainframes and email to steal data or disrupt business

- Other examples
  - Sexual harassment · Age/race/discrimination allegations
  - Expense account fraud
  - Stealing inventory and other company property
  - Misappropriation of confidential or proprietary information

*The information herein is of a summary nature and is limited to the U.S.; international rules and regulations may differ. It is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such, nor as financial, regulatory or legal advice which Kroll Associates, Inc. is not authorized to provide.

## II. The Search for Evidence: Where Supporting Evidence can be found

- Obtaining evidence under your control (subject to compliance with company policies, laws and regulations)
    - Image the subject's company desktop and/or laptop computers, Blackberry/handheld device to examine:
        - Email and Webmail
        - Word files, Spreadsheets
        - Calendars and Contacts files
        - Internet searches made by company employees
        - Search the unallocated space of the computer for deleted data
    - Suspend the deletion of data from the company server
    - Obtain:
        - Company telephone dial-out records to trace the subscribers of called numbers
        - Office card access records
        - Building visitor logs
        - Records of mailings from the company by the subject
        - Company expense accounts
    - Search the employee's office (subject to company policy and applicable law)
    - Audit vendor list for fictitious companies and undisclosed interests
- Evidence publicly available
    - Conduct a background investigation of the subject
        - Criminal and civil litigation
        - Judgments and Liens
        - Debt and bankruptcy
        - Business Registrations
    - Internet research - Investigations of hackers, defamers, extortionists and other abusers of the Internet
        - analyze metadata and internet service providers
- Interview prospective witnesses: employees, former employees and employers, vendors, customers and litigation adversaries

## III. Interviews

When conducting interviews:

- No more than two interviewers conducting the interview
- Interview conspirators simultaneously but separately
- Interview witnesses individually
- As a rule, do not tape record or videotape an interview
- Do not induce breach of NDAs

 

Interview Protocol

- Clearly identify who you are and that you represent the company (Upjohn v. United States, 449 U.S. 383 (1981).
- Make it clear that you are not the interviewee's lawyer or representative. (See United States v. Nicholas, No. SACR 08-00139-CJC, 2009 U.S. Dist. LEXIS 29810 (C.D. Cal. April 1, 2009; cited in "Cases Highlight Minefield in Internal Investigations", Lisa A. Cahill, New York Law Journal, May 21, 2009.)
- Affirm that everything that transpires during the interview is "on the record."
- Cooperation can be made a condition of continued employment
- Employees have a common law duty, and in many states, a statutory duty to answer questions regarding the performance of their jobs

Interviewing Targets

- Don't "bargain" or make concessions to a wrongdoer if you are holding good evidence
- Don't let the wrongdoer employee "think things over" overnight before answering questions
- If the subject has evidence to turn over, go with him/her to get it, even if it is outside the office (subject to legal advice.)
- Get a signed statement if possible

If you terminate an employee

- Notify Human Resources beforehand
- Notify vendors, company employees and the office building's management
- Disable or change the employee's passwords
- Cancel the employee's company credit cards
- Retrieve company owned property immediately

## IV. The Search for Evidence

Federal law · State law · Ethical considerations

Wiretapping · Recording of Conversations · Customer Records

- 18 USC 2511; NY Penal Law 250 et seq.
  Unlawful to intercept telephone communications (wiretapping) or "bug" a non-wire communication without consent of one party (some states require all parties' consent.)
- Consent
  Most states permit recording of conversations with one party consent; 13 states currently require all-party consent. *Kearney v. Salomon Smith Barney*, 137 p.3d 914 (Cal. 2006) California Supreme Court held that tape recorded calls to California made from Georgia violated California law
- Telephone Records and Privacy Protection Act of 2006 (TRPPA) 18 USC § 1039;
  New York Consumer Communication Records Privacy Act NY Gen Bus § 399-dd Cal PC 638
  Prohibits obtaining telephone records through deceptive means
- NY Penal Law § 250.30; Cal PC 538.5
  Prohibits use of deceptive means to obtain records
- Electronic Communications Privacy Act 18 USC 2510 et seq.
  Generally prohibits interception of communications, including email

Credit Records

- Fair Credit Reporting Act (FCRA) 15 USC § 1681 et seq. Prohibits obtaining credit records without a "permissible purpose" and consent. Permissible purposes include:
  - Pre-employment background check
  - Insurance application
  - Credit card application

 

- Judgment

Bank records

- Gramm-Leach-Bliley Act 15 USC § 6801 et seq. Prohibits obtaining customer information from a financial institution through fraudulent means.

Identity theft and criminal impersonation

- NY Penal Law 190.25: Criminal Impersonation.
  - Unlawful to impersonate another with intent to obtain a benefit
  - Unlawful to impersonate a public servant

## V. Responsibilities of Lawyers for Private Investigators

**New York Rules of Professional Conduct Rule 4.2(a)** (Effective April 1, 2009)

Communication With Person Represented By Counsel.

Rule 4.2(a) In representing a client, a lawyer shall not communicate or cause another to communicate about the subject of the representation with a party the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the prior consent of the other lawyer or is authorized to do so by law.

Lawyer's Responsibility For Conduct of Nonlawyers

Rule 5.3(a) A lawyer shall be responsible for conduct of a nonlawyer employed or retained by or associated with the lawyer that would be a violation of these Rules if engaged in by a lawyer, if:

(1) the lawyer orders or directs the specific conduct, or, with the knowledge of the specific conduct ratifies it;

"An attorney is responsible for the misconduct of his non-lawyer employee or associate if the lawyer orders or ratifies the conduct." Attorneys sanctioned where investigators contacted represented parties and recorded interactions with them.
*Midwest Motors v. Arctic Cat Sales, Inc*., 347 F.3d 693, 698 (8th Cir. 2003)

## VI. Ex Parte Communications

*Niesig v. Team 1*, 76 N.Y.2d 363 (1990)

Representation of a corporation does not extend to all employees for purposes of interviews. A "party" includes corporate employees whose acts or admissions in the matter are binding on the corporation or imputed to the corporation for purposes of liability or employees implementing the advice of counsel. All others may be interviewed informally.

*Muriel Siebert & Co., Inc. v. Intuit Inc.*, 8 N.Y.3d 506, 511 (2007)

"The policy reasons articulated in Niesig concerning the importance of informal discovery underlie our holding here that, so long as measures are taken to steer clear of privileged or confidential information, adversary counsel may conduct ex parte interviews of an

 

opposing party's former employee. Indeed, there is no disciplinary rule prohibiting such conduct."

## VII. Confidential and Undercover Strategies

Undercover investigations

- Investigations in which investigators assume the role of consumers can be lawfully conducted. *Gidatex, S.r.L. v. Campaniello Imports Ltd*., 82 F.Supp.2d 119 (SDNY 1999); *Cartier v. Symbolix*, 454 F.Supp.2d 175 (SDNY 2006); *U.S. v. Parker*, 165 F.Supp.2d 431 (WDNY 2001)
- "[h]iring investigators to pose as consumers is an accepted investigative technique, not a misrepresentation." *Gidatex*, 82 F.Supp.2d at 122
- "The prevailing understanding in the legal profession is that a public or private lawyer's use of an undercover investigator to detect ongoing violations of the law is not ethically proscribed, especially where it would be difficult to discover the violations by other means." *Apple Corps Ltd. MPL v. Int l Collectors Soc*., 15 F.Supp.2d 456, 475 (D.N.J. 1998)
- "Lawyers (and investigators) cannot trick protected employees into doing things or saying things they otherwise would not do or say… they probably can employ persons to play the role of customers seeking services on the same basis as the general public." *Hill v. Shell Oil Co.,* 209 F.Supp.2d 876, 880 (ND Ill. 2002)
- Ethical rules were violated where counsel was "integrally involved in the investigation." *Allen v. Int'l Truck & Engine,* 2006 U.S. Dist. LEXIS 63720 at 23 (S.D. Ind. 2006)

## VIII. Work Product Doctrine – investigators

The US Supreme Court recognized that the work product doctrine applies to investigators assisting attorneys in the compilation of materials for trial (denying application in the instant case on grounds of waiver.) *United States v. Nobles,* 422 U.S. 225, 239 (1975)

## IX. Choosing an investigations firm

- Research the background of the investigation company
- Confirm that the company is licensed in relevant jurisdictions
- Review the course of action proposed
- Make sure the proposed steps are lawful - question any strategy that sounds unconventional or wrong
- Don't use an internet service promising information on people finding and asset tracing
- Ask if the investigator will use subcontractors; assure that the investigator will supervise them and ensure compliance with law
- Don't hire investigators who boast of access to protected records such as credit reports and bank records

 

**Association of Corporate Counsel – Annual Meeting**

**Session 105**

**Conducting Corporate Investigations — The Use of Lawful and Ethical Strategies**

**Hypothetical Scenario for Discussion**

Panelists: Daniel E. Karson, John Lewis, Jr., Ralph C. Martin II, Marcia Narine

An Investigation at Consultate Corporation

Consultate Corporation is a publicly traded, multinational corporation with headquarters in the US. It is a diversified services company in the business of restructuring and organization consulting. Its clients are mostly manufacturers. Consultate develops its clients in large part through a network of non-employee sales representatives.

Consultate's "sweet spot" for the last 3 years has been advising companies in the developing world that are government owned but now are being privatized. Consultate uses several proprietary software programs in its consulting work. These programs are used by Consultate client managers in North America, Asia and Europe. While the large number of privatizations has helped Consultate's business, Consultate has also suffered some drop-off in other business sectors and has laid off some professional staff.

Richard Sarbox is Consultate's general counsel. He reports directly to the CEO of Consultate, but has a dotted line report to the chair of the Audit Committee of Consultate's board of directors.

On the morning of October 20, 2009 Sarbox opened an email from Gloria Fedsupp, the company's office manager in Albany, NY. In her email, Fedsupp told Sarbox that she had just received an anonymous email on her private Pseudomail account. (Pseudomail is a mass market free email service.)

The email read as follows:

**From:** gaga@pseudomail.com
**Sent:** Tuesday, October 20, 2009 7:00 AM
**To:** Gloria Fedsupp
**Subject:** Greetings

Hey Glo, how's it goin? Headquarters still RIFing you? Ya know how badly Consultate is paying you? I do! I got hold of everyones salary and bonus for 2008. Just check out the attachement. I might just email this to one of the business TV channels or blogs. Also, Im working for one of Consultates up and coming competitors – not telling ya who yet, and Im going after some of Consultates clients. Heck, with their software I can do the work for half what Consultate charges. Not worried about Consultate coming after me either. I know we only got that new Asian govt contract because our local guy and his rep paid off someone in the Ministry of Banking. Have a great life at Consultate!"

Seeya!

 

Sarbox read and reread the note. He confirmed that the attachment was an actual company spreadsheet containing accurate salary and bonus information (his was on the list.) Preliminarily he identified three issues:

- The writer, possibly an ex-employee had stolen proprietary salary and bonus information
- The writer had stolen proprietary software and was planning to give it to a competitor
- The writer had alleged that an agent of the company had paid a bribe to a foreign government official

Questions confronting the GC?

- Does Sarbox have any immediate legal obligation to report the possible FCPA allegation to law enforcement?
- Does Sarbox have any immediate legal obligation to inform Consultate employees that their salary and bonus information has been compromised?

Investigative Strategy?

- What first steps should Sarbox take to investigate?
- What internal records should Sarbox obtain?
- What requests for records and assistance should Sarbox make to Consultate's IT department?
- What investigative steps if any, should Sarbox take in Asia?
- Who should be interviewed first?

Pro-Active Investigative Strategies – What is permissible?

- May Consultate begin to secretly monitor employee email?
- May Consultate monitor employees' telephone conversations?
- May Consultate search employees' offices?
- May Consultate conduct background investigations of employees? Former employees?
- May a Consultate investigator "take over" Graham's Pseudomail account with Graham's consent and communicate with Gaga as if she were Graham, in order to get Gaga to respond and possibly provide clues or evidence?
- May a Consultate investigator contact Bankable, one of Consultate's competitors, pretend to be a new customer and see if Bankable's sales pitch sounds as if Bankable is using Consultate software?

Interviews

- Must Consultate investigators give "Upjohn" warnings to everyone they interview?
- How should Consultate respond if an employee asks to speak to a lawyer before answering questions?
- Consultate's HR department always sits in on employee interviews. Is there any downside to including them?

A week after the investigation began; Sarbox began to focus on 3 former employees of Consultate as suspects. He called in an assistant manager for an interview. The manager willingly answered questions about his work with the three former employees, but he refused to answer questions about his current contacts with them, or his knowledge of where they now were employed.

 

- May Sarbox compel the assistant manager to answer questions on penalty of dismissal?

The next day a current IT employee, Tanya Tech, was interviewed. Tech disclosed that she too received the list of employee salaries and bonuses, only her email came from former employee Mark Motherboard through a Pseudomail email account clearly identified with Motherboard's name. Consultate's investigators go to Motherboard's home and interview him. He admits to being the sender of the emails. He offers to give Consultate his hard drive in exchange for a promise of no prosecution.

- Sarbox reports Motherboard's offer to the CEO and the chair of the audit committee. The CEO wants to avoid the publicity that will come with an arrest of Motherboard. He tells Sarbox to make the deal. The chair of the audit committee disagrees, saying that such a deal is against public policy. May Consultate ethically and legally make such a deal?

 

## Association of Corporate Counsel – Annual Meeting

## Session 105

## Conducting Corporate Investigations in the U.S. — The Use of Lawful and Ethical Strategies

# Corporate Investigations: *Flagrante Delicto* and the Use of Undercover Strategies[1]

Daniel E. Karson
Kroll Associates, Inc.

In many investigations of crime, and misconduct, the best evidence of wrongdoing comes from an observation of the wrongful act itself. *Flagrante Delicto* is the archaic Latin term that describes one who is "caught in the act" or caught "red-handed". Certain investigations can be bolstered by obtaining information through an undercover type of inquiry.

For purposes of this discussion, an "undercover strategy" is one in which an investigator does not disclose his or her identity (and, in some cases, assumes a fictitious identity), either to make observations or to engage another person or persons in conversation. The purpose of the strategy is to obtain evidence of a crime, misconduct or civil wrong.

There are legal disagreements concerning the use of undercover strategies in private, non-governmental investigations. Law enforcement agencies and prosecutorial offices regularly use undercover type operations to obtain evidence in prosecutions of drug and illegal weapons trafficking, smuggling, conspiracies of various kinds, and many other categories of crime.

To what extent, though, may investigators retained by a private sector organization use an undercover strategy to obtain evidence in support of an investigation's objectives in the context of detecting fraud, misconduct, potentially criminal activity or other wrongdoing?

Some undercover strategies are so widely in use and so simple in application that no serious argument can be made in opposition. The most commonly known and utilized undercover strategy in the private sector is the purchase of counterfeit and gray market goods by investigators posing as consumers or retail vendors. Thus no one questions the right of the music, film, apparel and fragrance industries to purchase bootleg and counterfeit merchandise from street vendors and wholesalers. In the retail industry, the use of comparison shoppers to obtain information on prices, designs and presentations is in effect an undercover investigation (although in some contexts this may be distinguishable as competitive intelligence, rather than the detection of fraud or wrongdoing.)

The closer question concerns the application of undercover strategies in more complicated and in many instances, more serious cases, to obtain either direct or circumstantial

[1] **Disclaimer**: The information herein is of a summary nature and is limited to the U.S. International rules and regulations may differ. It is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such, nor as financial, regulatory or legal advice which Kroll Associates, Inc. is not authorized to provide.

 

evidence used in building a case regarding suspected fraud, other wrongdoing, either civil or criminal. The investigations corporate or external counsel now oversee cover a broad spectrum of topics. They include such divergent matters as the Foreign Corrupt Practices Act; USA Patriot Act; theft of intellectual property; Internet defamation; Internet extortion and computer hacking; unfair competition; embezzlement; theft of inventory; payment of kickbacks; tortious attempts to drive down a company stock price and various categories of discrimination and harassment, among others.

At their best, undercover strategies can establish proof of many crimes and civil wrongs. However, when abused or applied without due care and proper legal clearance, they may violate the law and ethical precepts. It is critical to consult counsel in evaluating potential methodologies on a case-by-case basis in light of the facts, circumstances, locations and issues in question.

The most recent notable example of the abuse of an undercover investigation was in 2006 when an investigator working for Hewlett Packard falsely impersonated HP board members and newspaper journalists. The investigator called a telephone company in order to obtain the records of the telephone numbers called by the people he was impersonating. This enabled the investigator to help identify the HP board member who had disclosed information to one of the journalists. The act of false impersonation was a crime, as was the obtaining of the telephone records. In the aftermath of the case, the investigator pled guilty to identity theft and conspiracy.

There are a number of U.S. laws and regulations relevant to undercover investigations. These include (with examples of federal and state statutes):

- 18 USC 2510 et seq re: "Wire and Electronic Communications Interception and Interception of Oral Communications" (prohibiting wiretapping telephone conversations or otherwise “bugging” a room to surreptitiously record conversations, the latter without prior disclosure or the consent of a participant (subject to the limitations noted) as well as intercepting email communications, and related state privacy laws prohibiting eavesdropping etc. (e,g, NY Penal Law Sec. 250 et seq.);
- State consent laws regulating the recording of telephone conversations[3];
- Federal and state laws protecting the privacy of telephone and consumer records and prohibiting obtaining the same through fraudulent means [4]
- Federal and state laws requiring a defined “permissible purpose” to obtain “consumer reports”[5]
- Federal financial privacy and safeguard rules protecting customer information and prohibiting obtaining customer bank account records through fraudulent means [6]
- Various state law prohibitions on false impersonation [7]

This is an illustrative list and should not be considered exhaustive. Other contemplated strategies may be prohibited by federal and state laws and even the laws of local governments.

[3] Most states permit recording conversations with the consent of one party to the conversation; 13 states prohibit recording a telephone conversation without the consent of all parties: California, Connecticut, Delaware, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania and Washington. *Cf* Kelly Kearney v. Salomon Smith Barney 2006 Lexis 8362. California Supreme Court held that tape recorded calls to California made from Georgia, a one party consent state, violated California law.
[4] Telephone Records and Privacy Protection Act of 2006 18 USC 1039; NY Gen. Bus. Law 399-dd; Cal PC 638; California PC 538.5
[5] Fair Credit Reporting Act 15 USC 1681 et seq and state analogues
[6] Gramm-Leach-Bliley Act 15 USC 6801 et seq
[7] E.g., NY Penal Law 190.25;

 

Counsel should always be consulted to ascertain the lawfulness of any investigative strategy.

Electing to Use Undercover Strategies

An undercover strategy may be a means of obtaining useful or needed evidence when either overt or other discreet strategies are unlikely to succeed or provide sufficient evidence. Undercover strategies require careful attention to the limits of law and ethics. In addition, they can be more labor intensive and expensive to deploy than other strategies.

In many investigations, particularly at a time when most information is communicated electronically, competent evidence can be found in locations under the dominion and control of a corporation, such as: company information technology systems – in company servers, computers and handheld devices; and in information databases – in online public records of business registrations, criminal proceedings, civil litigation, regulatory agencies and property records. Information not online may be found in local public record filings. Evidence may also be found through the accounts and testimony of witnesses.

However, complex investigations may require more thoughtful strategies. Evidence of corruption and other misconduct rarely appears on the surface. In certain cases, counsel may consider an undercover approach to uncovering evidence.

Ethical Considerations

More legal debate centers around the ethical considerations of undercover strategies than on violations of law. The difficult issue attorneys confront is whether the use of an undercover investigative strategy is in conflict with the prohibitions in codes of professional ethics against misrepresentations and deception, and communications with represented parties.

The leading case in point on the use of undercover strategies is Gidatex v. Campaniello Imports, Ltd.[8]

In *Gidatex*, attorneys for the plaintiff, a furniture manufacturer, hired private investigators to investigate a suspicion that the defendant, the plaintiff's former distributor, was making false statements about the plaintiff's brand and steering customers to other manufacturers.

Two investigators posed as customers and secretly tape recorded conversations they had with salespersons. The conversations produced the evidence sought by the plaintiffs.

Campaniello's attorneys moved to prevent Gidatex from offering its investigators' testimony and reports as evidence at trial, and also sought to exclude tapes made by the investigators. They alleged that Gidatex's attorneys had violated New York DR 7-102(A)(2)[9],

[8] 82 F. Supp. 2d 119 (S.D.N.Y. 1999.)

[9] Now Rules of Professional Conduct 8.4 (a). See also 5.3:
Responsibilities Regarding Non-Lawyer Assistants - With respect to a nonlawyer employed or retained by or associated with a lawyer:
(a) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;
(b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and
(c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:
(1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or

 

which prohibited attorneys from circumventing disciplinary rules through the actions of another and which also prohibits "conduct involving dishonesty, fraud, deceit or misrepresentation."[10]

The court held that the undercover strategy did not violate New York's rule against attorney misrepresentations, noting that "hiring investigators to pose as consumers is an accepted investigative technique, not a misrepresentation."[11] The Court concluded that ethical rules "should not govern situations where a party is legitimately investigating potential unfair business practices by use of an undercover posing as a member of the general public engaging in ordinary business transactions with the target."[12] The court found that rather than being unprofessional, "hiring investigators to pose as consumers is an accepted investigative technique."[13]

Campaniello similarly alleged violations of New York DR 7-104(A) (1)[14], which generally prohibited *ex parte* communications with represented parties. The court rejected both claims, citing New York's Court of Appeals ruling in Niesig v. Team 1[15], holding that the Campaniello salesmen were not "parties" within the meaning of the disciplinary rule:

> The New York Court of Appeals has defined "party" to include:
>
> corporate employees whose acts or omissions in the matter under inquiry are binding on the corporation (in effect, the corporation's "alter-egos"), or imputed to the corporation for purposes of its liability, or employees implementing the advice of counsel. All other employees may be interviewed informally. [16]

Moreover, the court concluded that the undercover strategy did not violate disciplinary rules. "Gidatex's investigators did not interview the sales clerks or "trick them into making statements that they otherwise would not have made." Rather, the investigators merely recorded the normal business routine in the Campaniello showroom and warehouse."[17]

In 1998, a New Jersey federal court determined that lawyers and/or their investigators, seeking to obtain information about corporate misconduct, could lawfully deploy undercover strategies in the form of an ordinary business transaction with low-level employees of a represented corporation.

In Apple Corps Limited v. Int'l Collectors Society,[18] the court considered whether plaintiff's counsel violated New Jersey's ethical rules in an investigation of alleged trademark infringement. During the investigation, plaintiff's law firm and its investigators contacted the defendant and posed as consumers attempting to purchase infringing products. Interpreting a

---

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

[10] Now Rules of Professional Conduct 8.4(c)

[11] Gidatex at 122

[12] Id.

[13] Id.

[14] Now Rules of Professional Conduct 4.2(a) *Transactions With Persons Other Than Clients*
Rule 4.2 Communication With Person Represented By Counsel
In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order.

[15] 76 N.Y.2d 363 (1990)

[16] Niesig 76 NY.2d at 374

[17] Id. at 126

[18] 15 F.Supp.2d 456 (D.N.J. 1998)],

 

rule similar to New York's DR 1-102(a) (4), the court found that the rule prohibiting deceit by an attorney "does not apply to misrepresentations solely as to identity or purpose and solely for evidence gathering purposes." "The prevailing understanding in the legal profession is that a public or private lawyer's use of an undercover investigator to detect ongoing violations of the law is not ethically proscribed, especially where it would be difficult to discover the violations by other means."[19]

In *Apple Corps Limited* the owners of Beatles trademarks, sued a stamp producer to enjoin unauthorized reproductions of the group's likenesses. After a consent decree was entered, the plaintiffs claimed the decree was being violated by the defendants.

The plaintiffs' counsel hired investigators to determine whether the defendants were actually violating the consent decree. The investigators posed as ordinary customers, and asked for and recorded recommendations about which stamps to purchase. Defendant's telephone salespeople offered and sold infringing Beatles stamps in violation of the consent order.

The plaintiffs then moved for contempt sanctions. The defendants cross-moved for sanctions on grounds that the investigators violated Rule DR 7-104(A) (1).

The court found no ethical violation, holding that New Jersey law only extended the protection of the rule to the company's litigation control group, and it was clear that the sales clerks did not fall within that group. The ex parte communications therefore were permissible.

With respect to the anti-deception provisions of Rule 7-102(A) (4), the court held that the investigators' misrepresentations about their identity and their purpose in contacting defendants were not a violation: "RPC 4.2 cannot apply where lawyers and/or their investigators, seeking to learn about current corporate misconduct, act as member[s] of the general public to engage in ordinary business transactions with low-level employees of a represented corporation. To apply the rule to the investigation which took place here would serve merely to immunize corporations from liability for unlawful activity, while not effectuating any of the purposes behind the rule."[20]

By comparison, in Midwest Motor Sports v. Arctic Cat Sales, Inc.,[21] the U.S. Court of Appeals for the Eighth Circuit found that plaintiff's counsel violated the "no contact" rule by hiring an investigator who secretly recorded conversations with the president and owner of a represented party, as well as with a salesman, about the subject of pending litigation. The court excluded all evidence obtained as a result of the recordings. The court relied upon the South Dakota Rules of Professional conduct, which were an adoption of the ABA Model rules[22].

*Midwest Motor Sports* involved a dispute concerning the discontinuance of the sale of a certain snowmobile line at the plaintiff's store. The defendant's investigator posed as a customer and recorded his conversations with one of the plaintiff's salesmen, during two separate visits to plaintiff's store, as well as a conversation with another snowmobile salesman at another party's store. Of particular importance to the court's decision was evidence that the investigator spoke with someone who had managerial responsibility in the organization that was represented by

[19] Id. at 474
[20] Id at 474-75
[21] 347 F.3d 693 (8th Cir. 2003)
[22] It held that the rules barred any contact with a represented company's employee's where the employee 1) has managerial responsibility in the represented organization, 2) his acts or omissions can be imputed to the organization for purposes of civil or criminal liability, or 3) his statements constitutes admissions by the organization. The court found that all the contacts made by the investigators fell within one or more of the relevant categories.

 

counsel; the defendant's attorneys instructed the investigator to record anything that the plaintiff's representative might say about the lawsuit; and the investigator admitted that his purpose in visiting the plaintiff's dealership was to elicit evidence for the pending litigation.

In In re Gatti,[23] the court concluded that such activities, even when undertaken by government attorneys seeking to deter criminal conduct, would constitute ethical violations.

In *Gatti,* the Oregon state bar instituted disciplinary proceeding against an attorney who allegedly posed as a medical doctor in telephone calls to an insurance company he was preparing to sue. Previous to this incident the same attorney had complained to Oregon Bar Counsel about the activities of local prosecutors who had supervised an undercover investigation into suspected workers' compensation fraud (directing investigators to pose as injured workers) that resulted in an indictment against one of his clients.

The bar counsel concluded that the prosecutors did not act unethically in providing advice in how to conduct a legal undercover investigation[24]. When the subsequent complaint was filed regarding the lawyer's alleged misrepresentation of himself as a doctor, the lawyer relied on the bar counsel's response to his earlier complaint and asserted that it was reasonable for him to infer from the bar counsel's response that it also was ethical for private attorneys to use undercover or deceptive methods to investigate other private parties[25].

The court rejected this argument, although the U.S. Department of Justice and numerous other amici (including many consumer organizations) urged the court to recognize an exception to Rule 8.4 for undercover investigations. The Oregon Supreme Court concluded that there was no investigative exemption from the disciplinary rules for lawyers who authorized or personally engaged in undercover activities involving deceit or misrepresentation.

The *Gatti* decision impacted only Oregon attorneys. It was quickly addressed by an amendment to the Oregon legal ethics rules, which became effective January 3, 2002. Oregon DR1-102(d) was amended to provide: "It shall not be professional misconduct for a lawyer to advise clients or others about or to supervise lawful covert activity in the investigation of violations of civil or criminal law or constitutional rights, providing the lawyer's conduct is otherwise in compliance with these rules." "Covert activity" was defined as "an effort to obtain information on unlawful activity through the use of misrepresentation or other subterfuge."

A 2007 opinion by the New York County Lawyer's Association ("NYCLA")[26] addressed the undercover strategy issue. The opinion expressly recognized and approved the holdings in *Apple* and *Gidatex* as ethically permissible, but only in a "small number of exceptional circumstances," including investigations of civil rights and intellectual property rights violations.

The opinion cited the Disciplinary Rules in the predecessor Code of Professional Responsibility then in effect in New York, the relevant content of which is largely replicated in the current Rules of Professional Conduct, which went into effect in New York, April 1, 2009[27].

The opinion begins by introducing the concept of "dissemblance." It defines dissemblance as: "To give a false impression about (something); to cover up (something) by

[23] 8 P.3d 966 (Or. 2000)
[24] Id. at 969
[25] Id. at 972
[26] NYCLA Committee on Professional Ethics Formal Opinion No. 737, 5/23/07
[27] E.g. DR 7-102(a)(5), now Rule 4.1 prohibits an attorney from "knowingly making a false statement of law or fact".

 

deception (to dissemble the facts)", citing Black's Law Dictionary[28]. The opinion distinguishes "dissemblance" from "dishonesty, fraud, misrepresentation, and deceit," stating that "…dissemblance refers to misstatements as to identity and purpose made solely for gathering evidence...." However, the opinion balances its reasoning entirely on a dictionary's definition of an arbitrarily selected term and not on any statute or case law. Further, while the opinion cites the leading cases, it badly misreads Gidatex, clearly the leading case on the subject.

The initial premise of the opinion is important, because its findings and reasoning all flow out of it. The opinion states that while there is no bright line between dissemblance and dishonesty, it would appear to be one of the "degree and purpose of dissemblance"[29]. The opinion states that "[d]issemblance ends where misrepresentations or uncorrected false impressions rise to the level of fraud or perjury, communications with represented and unrepresented persons in violation of the Code . . . or in evidence-gathering conduct that unlawfully violates the rights of third parties."[30]

The opinion carves out an exception for government attorneys supervising law enforcement personnel.[31] It seeks to establish standards for non-government attorneys supervising non-attorney investigators employing a limited amount of dissemblance. It sanctions "dissemblance" as long as:

i. either (a) the investigation is of a violation of civil rights or intellectual property rights and the lawyer believes in good faith that such violation is taking place or will take place imminently or (b) the dissemblance is expressly authorized by law; and
ii. the evidence sought is not reasonably available through other lawful means; and
iii. the lawyer's conduct and the investigators' conduct that the lawyer is supervising do not otherwise violate the Code (including, but not limited to, DR 7-104, the "no-contact" rule) or applicable law; and
iv. the dissemblance does not unlawfully or unethically violate the rights of third parties.

The NYCLA opinion further adds, "the investigator must be instructed not to elicit information protected by the attorney-client privilege."[32]

The opinion concludes that

"…it is generally unethical for a non-governmental lawyer to utilize and/or supervise an investigator who will employ dissemblance in an investigation if the dissemblance is unlawful; rises to the level of fraud or perjury; unlawfully violates the rights of third parties; otherwise violates the Code, or where other lawful means of obtaining evidence is available. Nevertheless; under certain exceptional conditions as set forth in this opinion dissemblance by a non attorney investigator supervised by an attorney is ethically permissible. Lawyers who supervise investigators employing dissemblance, however, should interpret these exceptions narrowly."[33]

Anchoring its opinion to the non-legal term *dissemblance* is odd (in contrast to "dishonesty, fraud, deceit or misrepresentation" specified in the actual Rule DR 1-102 A 4[34]. The opinion cites no statute or case in which the word is applied to the scrutiny of an

[28] 8th ed. 2004
[29] Id.at 2
[30] Id at 2-3
[31] Id at 3
[32] Id at 5-6
[33] Id at 6
[34] Now NY 8.4 (C)

 

undercover strategy. Instead it characterizes all such strategies as acts of "dissemblance." It does cite the *Gidatex* and *Parker* cases as sanctioning "dissemblance in investigations", but rejects their conclusions as "dicta."[35]

The opinion then arbitrarily carves out the two exceptions noted above, again without citing any particular authority for their selection. It is not clear why the opinion distinguished these categories from a host of others of no less importance in cases where businesses were defrauded or subjected to extortion, fraud or various computer crimes.

In addition, in an era where crimes against business are more sophisticated and can cause more devastating damage to companies, the limitation of undercover strategies, with a carve-out for law enforcement agencies and arbitrarily chosen categories for the private sector is counter-productive and counter-intuitive. Law enforcement agencies frequently do not have the resources available to respond to all threats made to businesses, either technologically or in staffing. They often must triage, and respond to situations where life or property is in imminent danger, or where the level of potential loss is greatest.

On the other hand, it is increasingly common for businesses to conduct their own investigations and turn over the findings to prosecutorial offices, particularly where the subject of the investigation is an economic loss in the low millions of dollars or less. Similarly it is not uncommon for a law enforcement agency or regulator, when notified by a corporation of the discovery of a criminal act, to permit the corporation to conduct its own investigation and ask that the corporation advise the agency of the investigation's progress and findings. To deny businesses the same investigative tools used by law enforcement further frustrates efforts by companies to defend themselves, and strains the resources of law enforcement agencies.

A better standard by which to measure the conduct of an undercover strategy would be: 1) does the strategy contemplated comply with the law?; and 2) is the information being sought through the undercover strategy otherwise publicly available to anyone else inquiring in the ordinary course? Of course the ethical rule that governs communicating with parties represented by counsel should override either consideration, noting, however, that in several jurisdictions, there are exceptions to this rule as well.

As reflected here and in other commentaries on the subject, the principal cases examining undercover strategies deal with what up to now has been their most common use – cases involving investigators posing as customers. However, changes in national and international commerce and Internet technology have required new applications of undercover strategies. Investigators have posed as company executives to "negotiate" with Internet extortionists who have invaded or threatened to invade IT systems. Investigators have assumed the identity of investors joining chat rooms to identify persons disseminating recklessly false information. They also have used these strategies to identify business entities used as covers for the payment of unlawful kickbacks, and to trace the source of pirated films. These are just a few examples of undercover strategies used to solve contemporary crimes against business.

With the few exceptions cited notwithstanding, most courts that have adjudicated the use of undercover strategies have supported their use, where the intent is to obtain the best evidence of misconduct or crime[36]. At the same time, there is no question that lawyers who

[35] Id. at 4
[36] See also "Privilege and Ethical Limits on Investigations in Trademark Cases" Peter Harvey

 

supervise investigations and investigators will be deemed legally and ethically responsible for the instructions they give.

To: All Consulate Employees

From: Consulate CEO

Subject: Principles of Business Conduct

We employees and shareholders of Consulate can take great pride in our Company's long heritage of following the highest standards of corporate governance and ethical business practices. This is especially true during these times when other companies are challenged with violations of laws or are struggling to put in place the types of practices that Consulate has followed for years.

Maintaining these high standards of governance is important to our continued growth and success. We all must take seriously our responsibility to ensure that our Company conducts business fairly, honestly and ethically – in good times and in bad – and at all levels of the organization. These are the values that Consulate's foundation was built on and that continue to set us apart in the marketplace.

Although it's important that we grow our business, we cannot do so at the expense of violations of the law or through unscrupulous dealings that undermine our reputation.

To that end, we are reinforcing our commitment to ethical business practices by expanding and revising Consulate's Principles of Business Conduct. The Principles apply in every location in which we do business around the world, as well as to every employee, officer, director and member of our Board of Directors. A complete text of the Principles of Business Conduct will be distributed at every location within Consulate and can also be found on the Consulate intranet site or the www.Consulate.com website. Country-specific codes are distributed as well, which have minor differences to account for legal requirements in our international locations.

The revised edition of our Principles sets forth enhanced reporting mechanisms and additional channels for employees, customers or vendors to confidentially report questionable business practices. It also includes Frequently Asked Questions and Integrity Inquiries designed to assist you in your daily efforts to uphold the Company's standards.

If a situation occurs that raises a question in your mind about legal or ethical compliance, you should immediately report it to any manager; to Human Resources; to Global Compliance at 1-800-62-CONSULATE, or ethics@Consulate.com; the Law Department, or to the Vice President of Audit Services. You can make a confidential and anonymous report through the Consulate HOTLINE at 800-815-2830, 24-hours a day, seven days a week. Employees who communicate concerns will not experience any retaliation or retribution.

I am proud of Consulate's strong values and ethical foundation. We all must strive to maintain our reputation for integrity and high ethical standards. Leading with integrity creates an environment for growth and success. The Consulate reputation belongs to all of us, as does our responsibility to protect it.

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

 

# OVERVIEW OF THE PRINCIPLES OF BUSINESS CONDUCT

This Overview will help you become familiar with the Principles of Business Conduct. The Overview is provided for your convenience, but you are expected to read and abide by the policies outlined in the full text of the Principles as a condition of your employment. If you have any questions, contact your supervisor, Human Resources, or Global Compliance at (800) 62-CONSULATE or at ethics@Consulate.com. The Principles apply in every country in which we do business, and to every employee, officer, director, and member of the Board of Directors (each country has a customized version as well). Every employee has the right and the obligation to promote ethical conduct, and to report known or suspected violations of the Principles, Consulate policy, or the law.

## REPORTING MECHANISM AND POLICY AGAINST RETALIATION

If you reasonably believe that a violation has occurred, you **must** report it immediately to your supervisor, Human Resources, any manager, the Global Compliance group at (800) 62-CONSULATE, or the Vice President of Audit Services at (305) 500-4255, and you may do so confidentially. You may make a confidential and anonymous report through the Consulate HOTLINE at (800) 815-2830, 24 hours a day, seven days a week, or by completing a report through Consulate.com. There are no tracking or tracing mechanisms, such as caller ID or other email identifiers. The reporting mechanisms are available to customers, suppliers, vendors, or anyone who has information about a suspected violation. **Consulate forbids retaliation against any employee who files a good faith report. If you believe that you have experienced retaliation, contact any manager, human resources or the Global Compliance Group.**

## EQUAL EMPLOYMENT OPPORTUNITY POLICY

Employment, recruitment, hiring and placement, compensation, benefits, promotion, training and termination at Consulate are based upon personal capabilities and qualifications regardless of: age, race, color, national origin, gender, gender identity or expression, sexual orientation, religion, disability status, veteran status, and any other status protected by law. The Company is committed to the principles of freely chosen employment, child labor avoidance, fair working hours, freedom of association, compliance with wage and hour laws, and humane treatment. If you believe that someone has violated this policy, contact any supervisor (even outside your chain of command, if that makes you more comfortable), human resources, or the Global Compliance Group. Any employee willfully violating this policy may be subject to appropriate disciplinary action, up to and including termination.

## OPEN DOOR PROCESS

You may raise any work-related concerns with any member of management without fear of retaliation. It is important that human resources and all appropriate levels of management have an opportunity to review your question, suggestion or complaint. However, if you do not feel comfortable speaking with your supervisor, you may skip that person and go directly to the next level or to any Consulate manager.



 

## CONFLICTS OF INTEREST

A conflict of interest may occur when an individual's personal interests interfere or appear to interfere with Consulate's interests. Perceived conflicts of interest can be as damaging as actual conflicts.

***Gifts*** – You may accept or provide nominal gifts or entertainment worth less than $100.00 if it does not influence, or have the appearance of influencing, objective decision-making; occurs infrequently; arises out of the ordinary course of business; involves reasonable, not lavish, expenditures; does not violate the other party's company's policies; and takes place in settings that are reasonably appropriate and fitting to you, your hosts or guests, and the business at hand. Notwithstanding the provisions of our Gifts policy, it is never appropriate to offer or provide gifts or other favors to a government official or employee regardless of the value of the gift or favor.

***Financial Interests/Investment in Other Companies –*** You must ensure that your financial interests do not create conflicts, as it relates to ownership of securities, participation in financial offerings or accepting loans.

***Providing Services to Other Companies, Including Your Own –*** You should not serve as an advisor, consultant or employee of a customer, supplier, vendor, or competitor of the Company (unless the Company is being paid for these services), without written approval. You may provide services to other companies such as a not-for-profit organization or your own business, but you must first receive approval from your management to ensure that there is no actual or apparent conflict of interest or violation of the Company's confidentiality policies. The Company will generally not hire your company or that of a family member to serve as a vendor to Consulate.

***Working With Family Members and Others With Whom You Have A Close Personal Relationship/Nepotism –*** Working relationships between family members and close, personal friends will be evaluated as to the potential to cause an actual or apparent conflict of interest or the perception of impropriety. You must disclose these relationships to management and human resources for guidance and possible work reassignment. Further, you must ensure that your personal relationships do not interfere with your business responsibilities as it relates to inappropriate reporting relationships or providing business opportunities to them.

***Insider Trading*** – The Company complies with the insider trading laws, which prevent the purchase or sale of securities based on the possession of material, nonpublic information. This information could concern Consulate, our customers or even other companies. You must not make investment decisions or trades based on non-public information if there is a substantial likelihood that the information would have an impact on the price of the Company's stock, or if a reasonable investor would consider the information important in making an investment decision. You do not have to be an executive to engage in insider trading. You should also not provide tips to friends or relatives based on material, nonpublic information.

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

 

## BRIBERY AND CORRUPTION/ TRADE RESTRICTIONS/EXPORT CONTROLS, ANTI-BOYCOTT AND ANTI-MONEY LAUNDERING

Consulate develops and maintains good relationships and effective communications with all levels of government in all areas in which we conduct business, and complies with all domestic and international anti-bribery laws such as the Foreign Corrupt Practices Act. The Company also complies with all laws related to Trade Restrictions and Export Controls, the U.S. Anti-Boycott Act, and Anti-Money Laundering and Office of Federal Asset Control provisions related to doing with business with known or suspected terrorists or illegitimate sources of funding.

## CONFIDENTIAL OR PROPRIETARY INFORMATION

Both during and after your employment with the Company you may not disclose, copy, sell or distribute Consulate's confidential and proprietary information to any third party, or any other Consulate employee (unless it is on a "need to know" basis). When you leave the Company, you must immediately return all Consulate-related information, equipment and property in your possession. Employees who reveal confidential information are subject to immediate and appropriate discipline, up to and including termination, and when appropriate, legal action. You also should not engage in unauthorized copying or reveal or encourage others to reveal or use any trade secrets of a former employer or other competitor in connection with your Consulate employment. The Company complies with the applicable privacy and data protection laws in the countries in which we operate.

## ENVIRONMENTAL POLICY

Consulate supports the important goals of sustainable development, environmental protection, and pollution prevention in its business of providing transportation and logistics solutions around the world. Employees have a responsibility to stay informed about environmental policies and programs and to take immediate corrective action to address any adverse situation or condition.

## ANTITRUST AND FAIR DEALING POLICY

You must deal fairly with Consulate's customers, suppliers, competitors and employees. No one should take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair-dealing practices. Never engage in activities with customers, suppliers or competitors such as bid rigging, market allocation, group boycotts, production agreements or price fixing that unfairly prevent or limit competition, or could appear to do so. Never engage in independent actions with respect to customers, suppliers or competitors that unfairly restrain trade and/or attempt to improperly gain market share.

## DOCUMENT RETENTION AND DESTRUCTION POLICY

The Company complies with all laws related to records retention. Wrongful destruction, alteration or falsification of records may subject the persons involved and the Company to civil liability and criminal penalties. ***Consult the Principles of Business Conduct for more detailed guidance on all of the policies listed above***.

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

 

# KEY PRINCIPLES

Consulate expects you as an employee to conduct business according to the highest ethical standards of conduct whether or not such action is required by the law.

## SHARED ACCOUNTABILITY FOR COMPLIANCE WITH THE LAW AND ETHICAL STANDARDS OF BUSINESS CONDUCT

The Principles of Business Conduct ("Principles") is a guide to the Company's compliance structure, applicable laws, and key policies and procedures that govern doing business in a legal and ethical manner. These Principles do not cover every situation that you are likely to encounter, but they do address those that are most important to the Company, as well as new regulations and policies that have been added since the last distribution of the Principles.

To help you determine whether you are or are not taking the proper course of action, we have included some of the most frequently asked questions and answers after each Principle. If you need additional guidance, we will tell you whom to contact.

If you have doubts about your course of conduct, ask yourself the following questions:

- Could your actions harm Consulate's reputation?
- Is it ethical and legal?
- What would your family and friends say?
- How would it look in the newspaper?
- Would you bet your job on it?
- Should you check with someone else?
- How would your actions appear to others?

The Principles of Business Conduct apply in all countries where we conduct business, unless otherwise prohibited by local law. All employees are subject to the laws and regulations of the locations where they work as well as to country-specific codes of conduct, but because Consulate is a global company, other laws may apply as well, and separate codes of conduct may exist. In some instances, U.S. law might apply to conduct that occurs outside the country for example, in the case of anticorruption and bribery and insider trading laws. If you are unclear about which policies and regulations apply to your activities, be sure to consult with your manager, your human resources representative, the Global Compliance Group, a Consulate lawyer, or, when appropriate, the Internal Audit Services Department. Contact information is available at your location, on Consulate.com and on Consulate's intranet. In addition, the Company will provide training to employees to ensure that you are aware of your compliance and ethical obligations.

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

 

Although the Company has established formal mechanisms to ensure that we comply with regulations and policies, Consulate views all employees as critical to maintaining an effective compliance system. In addition to your personal responsibilities for following the standards described in these policies, you are responsible for raising concerns about risks to the Company before these risks become actual problems.

All Consulate employees are required to report suspected or known violations of policy or the law. If you become aware of any suspected or known wrongdoing, you must abide by the following procedure:

File a report by contacting the Hotline at (800) 815-2830 in the U.S. and Canada or through an AT&T operator from international locations. A HOTLINE representative will answer your call and listen to your concerns. You may be asked follow-up questions to gather additional information in support of your report. At the end of your call, you will be given a callback date and code number to reference your call. Following your call, a written report is prepared based on the information you provided. This report is then forwarded confidentially to Consulate for review, investigation and response, as appropriate.

These calls are confidential and can be anonymous. You may also contact one of the following departments instead:

| Issue | Notification Requirement |
|---|---|
| Safety, Security, Theft, Violence | Safety Manager; Lotus Notes Security Incident Database |
| Workplace Conduct, Discrimination, Harassment, Employee Relations Issues, Time card abuse | Contact Human Resources |
| "Kickbacks," Financial/Accounting Improprieties, Fraud, Bribes | Contact the Internal Audit Services Department at xxxx, or email **audit@Consulate.com** to contact the Audit Committee of the Board of Directors |
| Legal Violations (i.e., antitrust; insider trading; corruption; breach of confidentiality; trade secret theft; privacy) | Contact Global Compliance. Contact Chief Privacy Officer at 800-62-CONSULATE or ethics@Consulate.com for potential breaches of customer or employee data (e.g. laptop or computer theft) |
| Conflicts of Interest (i.e., improper gifts and loans; investment in or providing services to other companies; nepotism) | Contact Global Compliance |

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

 

Strict procedures are in place to protect your identity, if you desire such protection. You may make anonymous reports; however, it may not be possible to fully investigate your concerns without some identifying details about your allegations, even if you do not disclose your name. All reasonable attempts will be made to investigate every claim as thoroughly as possible.

**CONSULATE FORBIDS RETALIATION AGAINST ANY EMPLOYEE WHO FILES A REPORT BASED ON HIS OR HER REASONABLE BELIEF THAT AN ACTUAL OR SUSPECTED VIOLATION OF THESE PRINCIPLES HAS OCCURRED OR IS ABOUT TO OCCUR. IF YOU BELIEVE THAT YOU HAVE EXPERIENCED RETALIATION BECAUSE YOU HAVE FILED A REPORT IN GOOD FAITH OR BELIEVE YOU ARE A "WHISTLEBLOWER", IMMEDIATELY CONTACT ANY MANAGER, HUMAN RESOURCES OR THE GLOBAL COMPLIANCE GROUP.**

Employees who file malicious or intentionally false reports of a violation of these Principles and employees who have knowledge of, but fail to report a violation will be subject to disciplinary action, up to and including termination.

Consulate will investigate any suspected violation of these Principles, including the failure to report a violation. If appropriate, law enforcement authorities will be notified. The Company supports criminal prosecution of those involved in any violation of these Principles that constitutes criminal conduct, regardless of restitution. This support will specifically include, but not be limited to, complete cooperation with respect to the availability of witnesses, documents and any necessary financial expenditures. In addition, when appropriate, the Company will institute civil and/or criminal proceedings against violators of these Principles.

## PROCEDURES FOR WAIVERS OF THESE PRINCIPLES

These Principles of Business Conduct apply to all Consulate officers, employees and members of the Board of Directors. There shall be no waiver of any part of these Principles for members of the Board of Directors or any employee, except by a majority vote of Consulate's Board of Directors or its Governance Committee, which will ascertain whether the waiver is appropriate and will ensure that the waiver is accompanied by appropriate controls designated to protect Consulate. Although the Board cannot conceive of any circumstance under which a waiver would be granted, in the extraordinary event that a waiver is granted, the waiver will be posted on Consulate's website and shall be disclosed in a public filing made with the Securities and Exchange Commission.

**All employees and members of the Board of Directors must comply with these Principles. In addition to these Principles, the Chief Executive Officer ("CEO"), Chief Financial Officer ("CFO") and senior financial management must comply with an additional code of ethics outlined below.**



 

## CODE OF ETHICS FOR CHIEF EXECUTIVE OFFICER, CHIEF FINANCIAL OFFICER, AND SENIOR FINANCIAL MANAGEMENT

The CEO, the CFO, and all senior financial management are responsible for full, fair, accurate, timely and understandable disclosure in the periodic reports required to be filed by the Company with the Securities and Exchange Commission (the "SEC").

Accordingly, it is the responsibility of the CEO, CFO and each senior financial manager to promptly bring to the attention of the CEO and/or the CFO, as appropriate, any material information of which he or she may become aware that affects the disclosures made by the Company in its public filings.

In addition, the CEO, the CFO, and each senior financial manager will assist the Company's Disclosure Committee in fulfilling its responsibilities to assure the accuracy and completeness of the Company's periodic reports.

The CEO, the CFO, and each senior financial manager shall promptly bring to the attention of the Disclosure Committee and the Audit Committee any information he or she may have concerning:

(a) significant deficiencies in the design or operation of internal controls which could adversely affect the Company's ability to record, process, summarize and report financial data, or

(b) any fraud, whether or not material, that involves management or other employees who have a significant role in the Company's financial reporting, disclosures or internal controls.

The CEO, the CFO and each senior financial manager shall promptly report any information he or she may have concerning:

(a) any violation of the Company's Principles of Business Conduct, including any actual or apparent conflicts of interest between personal and professional relationships, involving any management or other employees who have a significant role in the Company's financial reporting, disclosures or internal controls, or

(b) evidence of a material violation of the securities or other laws, rules or regulations applicable to the Company and the operation of its business, by the Company or any agent thereof.

With respect to the reporting obligations set forth in the previous paragraph, the CEO, the CFO and the Corporate Controller shall promptly bring the matter to the attention of the Audit Committee. Any other senior financial manager shall promptly bring the matter to the attention of (i) the General Counsel or the CEO or, if appropriate, (ii) the Audit Committee; provided, however, that while a senior financial manager always has the option of reporting directly to the Audit Committee, such person shall report to the Audit Committee if he or she has reason to believe that the General Counsel or CEO is involved with the matter at issue, or if he or she has reason to believe that the General Counsel or CEO has not addressed the matter appropriately in a timely fashion.



 

## CONSEQUENCES OF VIOLATING THESE PRINCIPLES

The Board of Directors or its designates shall determine appropriate actions to be taken in the event of violations of the Principles of Business Conduct or of the supplemental Code of Ethics by the CEO, the CFO, and the Company's senior financial managers. Such actions shall be reasonably designed to deter wrongdoing and to promote accountability for adherence to the Principles of Business Conduct and to this Supplemental Code of Ethics, and shall include written notices to the individual involved that the Board has determined that there has been a violation, censure by the Board, demotion or re-assignment of the individual involved, suspension, or when appropriate, termination of the individual's employment.

In determining what action is appropriate in a particular case, the Board of Directors or such designee shall take into account all relevant information, including the nature and severity of the violation, whether the violation was a single occurrence or repeated occurrences, whether the violation appears to have been intentional or inadvertent, whether the individual in question had been advised prior to the violation as to the proper course of action and whether or not the individual in question had committed other violations in the past.

## EXAMPLES OF VIOLATIONS OF PRINCIPLES OF BUSINESS CONDUCT

As an employee, you are expected to know the legal, policy, and financial controls that apply to your job. You are responsible for keeping accurate financial records for all of your transactions and business assessments, understanding the financial records and processes associated with your job, and protecting the Company assets and information that are entrusted to you.

You are forbidden to use, authorize or condone the use of "off book" bookkeeping, unauthorized accounts, unrecorded bank accounts, "slush funds," falsified books or any other device which could distort records or reports of the Company's true operating results and financial condition. The following are examples of improper practices requiring reporting:

- *Actions that could harm Consulate's reputation as an ethical company*
- *Financial records that don't accurately reflect the nature of the transaction*
- *Pressure for certain accounting results*
- *Efforts to avoid standard review and control processes*
- *Lack of periodic reviews of financial practices, records and results*
- *Poor record retention practices*
- *Failure to appropriately carry out duties regarding custody for recording and approving transactions affecting the Company's assets*
- *Financial results that do not match underlying performance*
- *Funds that have not been reported or assets that have not been recorded*
- *Transactions that lack the proper supporting documentation*
- *Lack of controls to protect physical assets from loss or impairment*
- *Estimates that are not supported by facts or appropriate documents*



 

- *Falsification of any reports*
- *Conversion to cash of checks made payable to the Company*
- *Misstatement of travel or expense reports or processing of non-business items for expense report reimbursement*
- *Engaging in any unethical act to entice a customer or potential customer to do business with the Company or another company*
- *Failure to report accurately the proceeds from the disposal of assets*
- *Acceptance of kickbacks*
- *Authorization for payment of goods and services not received, or over-payment for goods actually received or valid services performed*
- *Misuse of Company computer resources, including email and voice mail*
- *Unauthorized or improper access, misuse, modification, destruction or disclosure of Company data/software or non-Company data/software for which the Company has been identified as accountable for the processing, accessing and/or storing*
- *Delay in reporting expenses or revenues*
- *Failure to follow policies relating to capital expenditures*
- *Theft of Company equipment*
- *Using "workarounds" or schemes to avoid complying with domestic and/or international laws or policies*
- *Unauthorized use or disclosure of any confidential information or work product*
- *Inappropriate relationships among employees or between employees and vendors or customers that could pose a conflict of interests*

**FREQUENTLY ASKED QUESTIONS**:

**Q:** *I believe that my manager is stealing money from the Company. If I report this, how do I know that my contacts with the HOTLINE or ethics@Consulate.com will really be kept confidential? How can the Company guarantee that I won't face retaliation for making a report?*

**A:** You may provide your name to a Consulate HOTLINE specialist, but you are not required to do so. You will receive a control number so that you may call back for a follow-up report regarding the resolution of your report. The calls are not recorded and there are no tracing mechanisms. If you have a concern that you want to report anonymously online, Consulate.com will direct you to a screen that contains a form that you will complete online. That form will not list your email address and you do not need to identify yourself unless you choose to do so. Anonymous reports will be given the same priority as all other complaints. Any report made to ethics@Consulate.com or to any person designated to handle these reports will be handled with the utmost discretion.

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

 

## REPORTING VIOLATIONS OF THE PRINCIPLES OF BUSINESS CONDUCT

Consulate employees are expected to demonstrate the highest standards of business conduct in their relationships with other employees, customers, suppliers and the general public. You may call the HOTLINE 24 hours a day, seven days a week; make a report to the Global Compliance Group; report financial improprieties to the Audit Committee of the Board of Directors through audit@Consulate.com, or contact any manager, human resources or the Internal Audit Services Department at (305) 500-4255.

Consulate forbids retaliation against any employee who files a report based on his or her reasonable belief that a violation or suspected violation of these Principles has occurred or is about to occur. If you believe that you have experienced retaliation because you have filed a report, immediately contact any manager, human resources or the Global Compliance Group.

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

# EQUAL EMPLOYMENT OPPORTUNITY POLICY AND AFFIRMATIVE ACTION

***Integrity Inquiry: Are you saying or doing something to someone else that you would not want said or done to a member of your family?***

## EQUAL EMPLOYMENT OPPORTUNITY

Consulate is committed to Equal Employment Opportunity (EEO) throughout the workplace. Employment, recruitment, hiring and placement, compensation, benefits, promotion, training and termination of employment at Consulate are based upon personal capabilities and qualifications regardless of: age, race, color, national origin, gender, sexual orientation, gender identity or expression, religion, disability status, veteran status, and any other status protected by law. The Company is committed to the principles of freely chosen employment, child labor avoidance, fair working hours, freedom of association, compliance with wage and hour laws, and humane treatment.

If you have a question or concern regarding EEO, contact any Human Resources manager, or the Global Compliance Group. Any employee willfully violating this policy may be subject to appropriate disciplinary action, up to and including termination.

## AFFIRMATIVE ACTION

As a federal government contractor and/or sub-contractor, Consulate is required to have Affirmative Action Plans. These plans demonstrate the Company's commitment to hiring and promoting qualified minorities, females, covered veterans, individuals with disabilities and any other category as required by law.

The Senior Director of Global Compliance or his/her designate serves as the Company's affirmative action officer. This person can be reached through ethics@Consulate.com.



 

# POLICY AGAINST HARASSMENT, DISCRIMINATION AND RETALIATION

***Integrity Inquiry: When you see unfair or unethical treatment, are you stopping or reporting it? Are you seeing or allowing different standards in your organization?***

Consulate does not condone or tolerate harassment, discriminatory behavior or retaliation against individuals who report such behavior in good faith. Consulate's Policy against Harassment, Discrimination and Retaliation (HDR Policy) applies to harassment, discrimination or retaliation that occurs on Consulate premises or in some other location where Company activities occur, including Company or private parties where Consulate employees are present, informal lunches or gatherings, and vendor or customer sites.

Consulate will also ensure that people employed by its vendors, suppliers, customers and contractors adhere to the Policy, and that appropriate action is taken against those who harass, discriminate or retaliate against its employees.

## BEHAVIOR VIOLATING POLICY

Consulate supervisors and managers are held to a higher standard and are reminded that they represent the Company at all times both in and outside of the workplace. In circumstances where attending certain establishments offends our employees, tarnishes our Company's reputation, or alienates our customers or other business partners, the Company will take appropriate action.

Consulate strictly adheres to all federal, state and local laws governing harassment, discrimination and retaliation. However, there is a wide range of what could be considered inappropriate behavior under Consulate's HDR Policy even though such behavior may not be considered illegal.

The following examples are not intended to serve as a guide to what could legally be considered harassment, discrimination or retaliation, nor is this list intended to be all-inclusive. A violation of Consulate's Policy may lead to disciplinary action whether or not it violates the law.

## EXAMPLES OF BEHAVIOR VIOLATING CONSULATE'S POLICY

- Negatively affecting someone's employment because of a refusal to submit to sexual demands.
- Negatively affecting someone's employment on the basis of that person's age, race, color, national origin, gender, gender identity, sexual orientation, marital status, religion, disability status, veteran status or any other class protected by law.
- Engaging in the threat of or actual retaliation against any person who, in good faith, reports or files a claim of harassment or discrimination, or participates in internal investigations.
- Using degrading or stereotypical words or actions in jokes, cartoons, insults, tricks, pranks or horseplay related to age, race, color, national origin, gender, gender identity, sexual orientation, marital status, religion, disability status, veteran status or any other class protected by law.



 

- Circulating offensive or inappropriate emails, letters, etc.
- Using sexually suggestive or mocking comments that describe an individual's body or attire.
- Engaging in unwelcome sexual flirtation.
- Whistling or "cat calls."
- Making graphic or verbal commentary about an individual's body, sexual prowess or sexual deficiencies.
- Mocking, ridiculing or mimicking another's culture, accent, appearance or customs.
- Engaging in unwanted touching, grabbing, holding, kissing or hugging.
- Engaging in repeated "accidental" contact or other unwanted physical contact.
- Displaying sexually suggestive or provocative pictures or objects.
- Displaying an individual's actual physical body or parts of the body in a graphic manner.
- Staring or leering at a person's body.

## IF A POLICY VIOLATION OCCURS

If you believe that a violation of the Company's policy against harassment, discrimination or retaliation has occurred, you may, but are not required to, respond to the person causing the problem. Sometimes telling that person clearly and directly how you perceive the behavior, asking the person to stop, and letting the person know the consequences of continuing such behavior can rectify the situation.

You are nonetheless required to report offensive conduct to any manager, Human Resources or Global Compliance so that the Company can take the necessary steps to rectify the situation if the offensive conduct continues or you believe that the conduct is so severe or widespread that action must be taken.

Some disclosure of your allegations may be necessary to the person under investigation, witnesses or other key individuals. All efforts will be made to keep as much information confidential as possible.

**SUPERVISORS OR MANAGERS WHO WITNESS OR ARE INFORMED OF A POSSIBLE VIOLATION OF THE COMPANY'S POLICY AGAINST HARASSMENT, DISCRIMINATION OR RETALIATION ARE REQUIRED TO INTERVENE AND REPORT THE INCIDENT, WHETHER OR NOT THE INDIVIDUALS ARE IN THEIR CHAIN OF COMMAND. FAILURE TO DO SO WILL RESULT IN DISCIPLINARY ACTION, UP TO AND INCLUDING TERMINATION.**

## DISCIPLINARY PROCEDURES

If an investigation reveals that the alleged policy violation did occur, the offender will be subject to the appropriate disciplinary action, up to and including termination.

## FALSE REPORTS

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

 

If you knowingly make a false report against another employee, you will be subject to disciplinary action, up to and including termination.

However, if you report in good faith what appears to be a violation of our policy against Harassment, Discrimination or Retaliation—even if the reported incident is determined not to be a policy violation—you will not be subject to disciplinary action for making the complaint.

## AVOIDING INAPPROPRIATE BEHAVIOR OR CONDUCT

In order to ensure that all Consulate locations are free from inappropriate behavior or conduct, every employee and manager must fulfill the following requirements:

- Set an example by your own behavior and consistently treat others with respect and dignity.
- Do not use inappropriate language.
- Refrain from joking or bantering that might make others uncomfortable, even if it appears consensual.
- Remove any inappropriate, sexually suggestive or offensive pictures, calendars, screensavers or objects from your work place, including your computer.
- Report inappropriate graffiti.
- Do not attend adult entertainment establishments with Consulate employees, customers, vendors or business partners while on or discussing Consulate business.
- Do not make sexually suggestive comments.
- Intervene when others tell inappropriate jokes or tease someone in your work environment. Report the incident if necessary.
- Do not forward offensive or inappropriate emails to others, and inform senders not to send such emails to you at your workplace.



 

# AMERICANS WITH DISABILITIES ACT POLICY

Consulate is committed to complying with all applicable provisions of the Americans with Disabilities Act (ADA) as well as state law versions of the ADA.

## REASONABLE ACCOMMODATIONS

If you believe you have an ADA-defined disability and need reasonable accommodations to perform the essential functions of your job, contact your immediate supervisor.

Unless otherwise prohibited by law, Consulate will provide reasonable accommodations as long as:

- The accommodations do not constitute an undue hardship on the Company;
- You are able to perform the essential functions of your job with or without a reasonable accommodation; and
- Your working does not pose a direct threat to yourself or others.

**Note:** The ADA does not require Consulate to make the best possible accommodation, to reallocate essential job functions or to provide personal use items (e.g., eyeglasses, hearing aids, wheelchairs).

When appropriate, Consulate will work with you (and your healthcare provider, if necessary) on an interactive basis to develop an appropriate accommodation.

## QUESTIONS, INQUIRIES OR COMPLAINTS

If you have any questions regarding the implementation of the ADA or believe that you were discriminated, harassed or retaliated against based on a disability, notify your Human Resources manager or the Global Compliance Group.

Your inquiry or complaint will be treated as confidential to the extent permissible by law.



 

# OPEN DOOR PROCESS

***Integrity Inquiry: Are you telling management what they need to know so that they can address issues early on? As a manager, do you truly have an Open Door?***

As a Consulate employee, you may participate in the Company's Open Door Process. Through this process, you are guaranteed the right to talk about any work-related concerns with any member of management without fear of retaliation.

## CHAIN OF COMMAND

To best address your work-related issue, it is important that all appropriate levels of management have an opportunity to review your question, suggestion or complaint. The use of the chain of command ensures that the proper decision-makers are involved in the resolution decision. You should first address your issue with your immediate supervisor or your Human Resources representative. However, if you do not feel comfortable speaking with your supervisor, you may skip that person and go directly to the next level.

**If you believe that you cannot go through the chain of command, contact any manager, even if that person is not in your chain of command.**

Regardless of where you begin the process, Consulate's Human Resources Department is responsible for ensuring that your issue is resolved in a timely manner with the correct levels of management involvement.

**In situations involving a violation of ethics, Principles of Business Conduct, the law or the Company's Policy Against Harassment, Discrimination and Retaliation, you may contact any Human Resources manager directly or the Global Compliance Group. In these situations, the Company does not require that you follow the chain of command.**

## COMPANY POLICY ON RETALIATION

Company policy strictly prohibits retaliation against any employee who in good faith exercises legally protected rights or who utilizes the Open Door Process.

If at any time during or following the Open Door Process you believe that you are being subjected to retaliation, report it to your Human Resources manager or the Global Compliance Group. Upon completion of an investigation, anyone found to be responsible for retaliatory behavior is subject to disciplinary action, up to and including termination.

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

# CONFLICTS OF INTEREST

***Integrity Inquiry: Could your actions cause an employee, customer, vendor or other observers to believe that you are putting your interests above the Company's? Have you disclosed all potential or actual conflicts of interests, including vendor relationships and your personal side businesses?***

A conflict of interest may occur when an individual's personal interests interfere or appear to interfere with Consulate's interests. Perceived conflicts of interest can be as damaging as actual conflicts. It is difficult to list every possible circumstance that could give rise to a possible conflict of interest. Consulate has, however, established specific guidance in the following areas, where conflicts of interest most often arise:

1. **Gifts, Personal Loans and Offers To Perform Personal Services**
2. **Investments in Other Companies/Providing Services to Consulate as a Vendor**
3. **Providing Services to Other Companies/Board Positions**
4. **Working with Family Members and Others with Whom You Have a Close Personal Relationship/Nepotism**
5. **Insider Trading**
6. **Doing Business with the Government**
7. **Disclosure of Possible Conflicts of Interest**

**Note:** These standards apply to you and to your family members, which for the purpose of this policy, is defined as one of the following: spouse, domestic partner, child, parent (including in-laws), sibling, grandparent, grandchild, niece, nephew, cousin, aunt, uncle, roommate, relative residing at your home, anyone serving in the place of one of the previously mentioned family members, and in some circumstances, close personal friends.

## 1. GIFTS, PERSONAL LOANS AND OFFERS TO PERFORM PERSONAL SERVICES

***Integrity Inquiry: Are you causing a vendor or supplier to feel that they need to provide gifts or entertainment to get or keep Consulate business?***

It is never appropriate to ask for gifts, which can take the form of goods or services. From time to time, you may give or receive gifts that are meant to show friendship, appreciation or thanks to or from people who do business with Consulate.



 

You may also receive offers to provide services to you personally from vendors, employees, customers or others who want to do business with Consulate. These offers of personal service to you or your family members should be refused, and you should never ask others to perform these services for your personal gain.

Generally speaking, accepting or giving gifts, such as t-shirts, flowers, candy, items with logos or other nominal items is acceptable, provided that you do not ask for the gift and as long as it does not influence, or have the appearance of influencing objective decision-making.

It is generally inappropriate to give or accept: more than $100.00 worth of gifts to or from a single source in any twelve-month period; lavish entertainment; invitations to leisure trips that require overnight travel; or other benefits resulting in personal gain (e.g., preferential access to IPO's). Cash gifts are never appropriate.

The Company will consider many factors to determine the appropriateness of any gift over the $100.00 amount including, but not limited to whether:

- the gift is customary or industry appropriate and openly given without any expectation or realization of special advantage;
- several people received the same gift (i.e., gifts for speakers on a panel);
- it was a raffle prize; or
- the gift is clearly advertising or promotional material marked with the company's name or brand names.

You may accept or provide entertainment if:

- it occurs infrequently and arises out of the ordinary course of business;
- it involves reasonable, not lavish, expenditures;
- it does not knowingly violate the other party's company's policies; and
- it takes place in settings that are reasonably appropriate and fitting to you, your hosts or guests, and the business at hand. The Company will not pay for any expenses at an adult entertainment establishment, and employees are prohibited from attending these establishments with Consulate employees, customers, vendors or other business partners while on or discussing Consulate business.

Personal loans to officers and members of Consulate's Board of Directors, or guarantees of such obligations, are prohibited. If you have questions about this policy, you should seek guidance from your human resources representative, an officer in your organization, or the Global Compliance Group.



 

**FREQUENTLY ASKED QUESTIONS:**

**Q:** *Can I give one of my customer's tickets to a sporting event?*

**A:** Giving tickets is acceptable if it's part of relationship management, it does not violate the customer's own policies, and if your manager provides approval in advance. If the customer is an official, employee or agent of a governmental official, contact the Global Compliance Group for guidance.

**Q:** *Can I accept a business meal from a customer or supplier? What about tickets to the Super Bowl or another high profile event?*

**A:** You may let a customer or supplier pay for a meal arranged for the purpose of discussing business. However, it is inappropriate to let customers or suppliers repeatedly pay for your meals. You should exercise extra caution if you are in the middle of negotiating a contract with a supplier, and that supplier offers to provide expensive tickets or other lavish entertainment. If you are offered extraordinary opportunities to attend a high profile event, you must get permission from Global Compliance or Human Resources.

**Q:** *One of our customers sent me an expensive gift basket for the holidays. Am I allowed to keep it?*

**A:** You may accept the gift if it is unsolicited, not lavish, and would not cloud or be perceived as clouding your business judgment. It may be wise to share the gift with members of your department, others within the Company, or donate it to a charity. If you have questions, consult with your manager or the Global Compliance Group.

**Q:** *One of our vendors offered me the use of his vacation home for a week. It costs him nothing, and Consulate had a long-term relationship with this vendor even before I started working for the Company. I am not personally involved in negotiating the contracts, and the vendor has not asked for any special treatment. May I accept this offer?*

**A:** Although the vendor has not asked for a favor in return, there could be an appearance of impropriety to the employees, the customer and/or other vendors. There may come a time when you have more influence or involvement in the award of contracts to this and other vendors; and therefore, you must avoid any actions that could lead others to believe that you would not be impartial.

**Q:** *One of my co-workers is having a bachelor's party at a club that seems to be prohibited under the policy. We won't be discussing work issues and we won't be requiring anyone who doesn't want to go to come to the party. Is this a problem?*

A. The Company is not attempting to legislate what employees do on their free time. However, you need to be aware that supervisors and managers are in a special position of authority, and represent Consulate at all times both in and outside of the workplace. Patronizing certain establishments with employees or business partners is considered inappropriate, even in purely social, non-business situations, when it could tarnish our Company's reputation, offend

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

our employees, or alienate our customers or other business partners. When considering whether to attend or hold a certain event, even at a more traditional venue, ask yourself the following questions:

1) Would other employees feel uncomfortable attending, or feel that they had no choice but to attend, to build relationships with clients, peers or Company management?

2) Would I want my attendance at this venue or event to be kept a secret from other employees?

3) Would I be uncomfortable if my name appeared in a news article about an incident that occurred at the venue or event?

## 2. INVESTMENTS IN OTHER COMPANIES/PROVIDING SERVICES TO CONSULATE AS A VENDOR

Employees may generally buy stock or hold investments in other companies, including companies that compete, do business, or are negotiating to do business with Consulate. If an employee, however, holds a substantial interest in a customer, supplier, partner, vendor, or competitor ("Partner/Competitor"), there may be a conflict between the Company's interests and the employee's financial interest.

As a general guide (but not limit), "substantial interest" is an ownership interest greater than 5% of the total net worth of the employee and immediate family members, or greater than 1% of the outstanding equity securities for investments in a public company. This policy does not apply to mutual funds or managed accounts in which the employee exercises no discretion as to the choice of investment.

Employees and those defined as "family" in this Conflicts of Interest policy are prohibited from providing services to Consulate as a vendor. Employees who currently serve as vendors or who have family members who serve as vendors must notify the appropriate Human Resources Manager and the Vice President of Global Compliance and Business Standards at 1-800-62 CONSULATE or ethics@Consulate.com immediately. A Vendor Disclosure Form, available on the intranet, must also be submitted. Failure to do so may lead to termination of employment and an immediate termination of the vendor relationship.

Consulate also prohibits employees from investing in a Partner/Competitor of Consulate's if, by virtue of your position with Consulate, you have access to material, nonpublic information about the Partner/Competitor or may be able to influence Consulate's decision to do business with them.

If you are unsure about whether a situation could result in a conflict of interest, ask for guidance from the Global Compliance Group.

### FREQUENTLY ASKED QUESTIONS:

**Q:** *My wife inherited an amount of our competitor's stock that would be considered "substantial" under the guidelines listed above. I have just become aware of the Company's policy. Does she have to sell it?*



 

**A:** The answer will depend on your position within the Company, among other factors. Although you do not own the stock yourself, your wife's financial interest could have the potential to influence your decision-making in a manner that is directly or indirectly adverse to Consulate's interests. Even if you have no such intent, the appearance of impropriety could harm the Company. You should contact the Global Compliance Group for guidance.

## 3. PROVIDING SERVICES TO OTHER COMPANIES/BOARD POSITIONS

There are serious responsibilities and obligations associated with becoming a member of any company's board of directors. These could include potential financial liability, time and travel commitments, public relations issues, and potential expectations of helping to make contacts within Consulate.

Therefore, you should not accept an invitation to become a board member of any company or organization unless you have received written approval from your manager, and your manager, if necessary, has obtained guidance from the Global Compliance Group. If you already are serving as a board member of another company, you should promptly seek approval from your manager and your manager should obtain guidance from the Global Compliance Group to continue in your board position.

### Other Services to Partner/Competitor/Consultant Companies

Given the potential for a conflict of interest, you should not serve as an advisor, consultant, employee of or vendor to a Partner/Competitor/Consultant of the Company (unless the Company is being paid for these services), without written approval from human resources and an officer in your organization. This includes providing primary market research information to those who advise on or cover our business, whether or not they have been retained by Consulate.

### Other Services to Other Companies / Managing Your Own Business

If there is no actual or apparent conflict of interest or a violation of the Company's confidentiality policies, and you continue to meet the performance standards of your job, you may provide services in any capacity not covered above, such as managing your own business. However, you must inform your manager of your outside business accounts to ensure that there is no potential problem. All employees will be judged by the same performance standard and will be subject to the Company's scheduling needs, regardless of any existing outside work requirements. If your outside work interferes with your performance or ability to meet the current requirements of your job, you may be asked to terminate the outside employment or involvement.

**FREQUENTLY ASKED QUESTIONS:**

**Q:** *I own my own catering business and want to provide services to Consulate employees, as well as the general public. I would not be competing with any of Consulate's business interests. Am I permitted to do this?*

**A:** Your outside business would not cause a conflict of interest provided that**:**

- you have received permission from your manager;
- you do not use Company resources or time to solicit business;
- your participation in the business is accomplished outside of your normal work hours; and



 

- your participation in the business does not adversely impact Consulate or your ability to do your job at Consulate. However, generally, you may not provide services to Consulate as a vendor.

## 4. WORKING WITH FAMILY MEMBERS AND OTHERS WITH WHOM YOU HAVE A CLOSE PERSONAL RELATIONSHIP/NEPOTISM

### A. Non-Platonic Relationships

At times, consensual romantic and/or sexual relationships or non-platonic living relationships between co-workers may occur. Such relationships between a supervisor and an employee in which the supervisor has the ability to impact the progress or assignments of another employee are strictly prohibited, even when there is no direct reporting responsibility. Similarly, the Company prohibits non-arms length relationships between employees who are not in a subordinate relationship but who are in a position of support or trust (e.g., Field Finance Director, Director of Customer Logistics, etc.).

Therefore, if such relationships arise, the supervisor or person involved is required to disclose the relationship to the Human Resources Department so that a change in the responsibilities of the individuals involved or transfer of location within Consulate can occur.

The Human Resources Department will work with the supervisor's and employee's management to determine the appropriate action. At a minimum, the supervisor must withdraw from participation in activities or decisions that may reward or disadvantage the employee, including decisions related to hiring, performance appraisals, promotions, compensation, work assignments and discipline. Such employees are not permitted to be in working relationships that could create situations that, in the Company's sole discretion, unduly influence their job performance or the performance of others. If no transfer or change is possible, one employee may be required to voluntarily terminate his or her employment with the Company. Whether or not the relationship has been disclosed, if you believe that you were penalized in terms of employment because of such a relationship, you should contact your Human Resources manager immediately.

### B. Family Relationships/Close Personal Friends

It is not unusual in companies the size of Consulate to have relatives working for the same company, and members of an employee's family will be considered for employment on the basis of their qualifications. Generally, this does not result in conflict. But sometimes, situations in this area can be troublesome. For example, it would be an inappropriate conflict for you to hire or seek to inappropriately influence another employee to hire a relative or member of your household. Similarly, it could be a conflict if you have a reporting or business relationship with employees who also work in the same area as a relative or member of your household.



 

Therefore, a family member, roommate, close personal friend (in certain circumstances), or an individual who is currently involved in a non-platonic relationship with a Consulate employee may not be hired in or support the same department or work group or continue to work in or support that group if it would create a supervisor/subordinate relationship with any individual described above; have the potential for creating an adverse impact on work performance of the employee or others; or reasonably create an actual conflict of interest, the appearance of a conflict of interest, or the perception of unfairness to other employees.

Depending on the circumstances, employees who become family members (through marriage, domestic partnerships or otherwise) may be prohibited from continuing in working relationships that would create one of the above conditions. This policy must be considered when assigning, transferring or promoting an employee. Any such situation should be reported to your Human Resources representative so that proper procedures can be followed.

It also could be a conflict if you, on behalf of Consulate, do business with another company in which you or a family member has a personal or financial interest. Any such situation should be reported to your supervisor and the Global Compliance Group for guidance and approval, and through the use of the Vendor Disclosure Form, available on the intranet.

**FREQUENTLY ASKED QUESTIONS:**

**Q:** *Am I allowed to date a woman/man who is not in my direct chain of command but who is in my department at a lower level or who provides support to my group?*

**A:** If you have the ability or potential to have an impact on his/her performance appraisals, promotional opportunities, salary adjustments, or continued employment, even in an informal or "off the record" capacity, you should not date the employee. Dating the employee could be a policy violation and could cause others to believe that s/he could receive preferential treatment from the Company. Such perceptions often lead to disruption in the workforce, poor morale, and reduced productivity.

**Q:** *I am in charge of hiring one of the vendors at our facility. My sister-in-law owns a business that provides a service that Consulate needs. We put the contract out for bid. She is competitively priced and has an excellent reputation in our city. Can I hire her firm?*

**A:** Although it appears as though you took steps to avoid a conflict of interests, unfortunately, there could still be the perception of favoritism. Generally, in this situation, the Company would not hire her firm.

## INSIDER TRADING



 

***Integrity Inquiry: Don't buy or sell stock based on nonpublic information about the Company, current or prospective customers or vendors. You don't have to be an executive to engage in insider trading under the law. Check on the intranet for the complete Insider Trading policy and with the Law Department if you have any doubts because the penalties for violation are severe.***

The Company has adopted an Insider Trading Policy (the "Policy") both to prevent insider trading and to help employees avoid the severe consequences associated with violations of the insider trading laws. The insider trading laws prevent the purchase or sale of securities based on material, nonpublic information.

It is illegal and against Company policy to directly or indirectly buy or sell Consulate's securities while in the possession of material, nonpublic inside information. The only exception is a purchase or sale made pursuant to a trading plan with your broker established under SEC Rule 10b5-1 that has been pre-approved by the Company. The same restriction applies to the purchase or sale of the securities of any other company. In particular, these restrictions apply to material, nonpublic information concerning Consulate's existing or potential customers, suppliers, competitors and business partners which you may acquire as part of your work for Consulate. It is also illegal to inform others, including family members, friends or other entities, about inside information or to make stock buying or selling recommendations to others based on such information.

The Securities and Exchange Commission ("SEC") and the United States Department of Justice vigorously pursue people who violate the insider trading laws and punish offenders severely. While the government typically pursues enforcement against the individuals who make illegal trades, or who tip inside information to others who trade, the Company or other "controlling persons" could be subject to potential liability for failure to take reasonable steps to prevent insider trading by employees.

This Policy also prohibits even the appearance of improper conduct by Board members, employees, employees of foreign subsidiaries or anyone else associated with the Company (not just so-called "insiders"). The same restrictions that apply to you, apply to your family members who reside with you, anyone else who lives in your household and family members who do not live in your household but whose transactions in Company securities are directed by you or are subject to your influence or control.

If you are aware of material, nonpublic information when your employment or service relationship with Consulate terminates, you still may not trade in Company securities until that information has become public or is no longer material.

Information is **material** if there is a substantial likelihood that the information would have an impact on the price of the Company's stock, or if a reasonable investor would consider the information important in making an investment decision. Any information that could be expected to affect the Company's stock price, whether it is positive or negative, should be considered material.

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

*Examples of material information would be: significant upward or downward revisions to earnings forecasts; significant restructurings; senior management or independent auditor changes; important product or litigation developments; mergers; acquisitions; tender offers; joint ventures; changes in control; gain or loss of significant customer or supplier; defaults on senior securities; redemption calls; repurchase plans; stock splits; changes in dividends or sales of securities; developments affecting major business units; and bankruptcies.*

**Nonpublic** information is information that is not generally known or available to the public. Information is considered to be available to the public only when it has (1) been released broadly to the marketplace (such as by a press release or an SEC filing), and (2) the investing public has time to absorb the information fully. As a general rule, information is considered nonpublic until the second full trading day after the information is released.

**Unauthorized Disclosure.** Maintaining the confidentiality of Company information is essential for competitive, security and other business reasons, as well as to comply with securities laws. You should treat all information you learn about the Company or its business plans in connection with your employment as confidential and proprietary to the Company both during and after your employment. Inadvertent disclosure of confidential or inside information may expose the Company and you to significant risk of investigation and litigation.

The timing and nature of the Company's disclosure of material information to outsiders is subject to legal rules, and if you violate those rules, you, the Company, and its management could be subject to substantial liability. Accordingly, it is important that responses to inquiries about the Company by the press, investment analysts or others in the financial community be made on the Company's behalf only through authorized individuals. Please consult the Company's Disclosure Policy for more details regarding the Company's policy on speaking to the media, financial analysts and investors.

## 6. DOING BUSINESS WITH THE GOVERNMENT – GIFTS AND ENTERTAINMENT

The federal and many state and local governments have very strict policies prohibiting the provision of gifts, entertainment, meals, favors or other things of value to government employees. These rules apply to the government's contractors and subcontractors as well. Activities that might seem customary or reasonable when dealing with private sector customers may be improper or illegal when dealing with governmental employees. Notwithstanding the provisions of our Gifts policy, it is never appropriate to offer or provide gifts or other favors to a government official or employee regardless of the value of the gift or favor.

If you are directly or indirectly involved in providing services or products to the government, there may be certain instances in which you cannot receive gifts, entertainment, meals or favors from your vendors or suppliers. You should apply these same rules when dealing with state or local governmental officials or agents as well, and you must be aware of applicable procurement, bribery and other laws. For more guidance on these issues, contact the Global Compliance Group or the Procurement Department.



 

**FREQUENTLY ASKED QUESTIONS:**

**Q:** *Can I invite a U.S. government customer to a working lunch?*

**A:** You may invite the person, but he or she would be required by government regulations to reimburse the Company for the meal.

## 7. DISCLOSURE OF POSSIBLE CONFLICTS OF INTEREST

Even if a situation is not covered by the guidelines above, it may result in a conflict of interest. If you find yourself in a situation that could cause a conflict of interest or the appearance of one, you are required to promptly inform your supervisor or any member of management so that the possible conflict and corrective action can be considered. If you do not wish to inform management, you may contact the Global Compliance Group directly.

### Related Party Transactions-Executive Officers and Board Members

In addition to the Conflicts of Interest Policy, the Company is governed by Securities and Exchange Commission ("SEC") regulations, which require public disclosure of certain specific transactions between a company and its executive officers, Board members, Board nominees, and their respective immediate family members (the "Related Parties"). Consulate's policy requires that any transaction between Consulate and Related Parties be pre-approved by the Board. The Company will comply with all SEC disclosure requirements.



 

# SAFEGUARDING CORPORATE ASSETS AND OPPORTUNITIES

Consulate entrusts you with numerous company assets. You have a special responsibility to protect those assets from loss, damage, misuse or theft. Consulate's assets include financial assets, buildings, equipment, supplies, the time it pays you to work and much more. Consulate assets are to be used for the benefit of Consulate and not for personal gain.

Employees and members of the Board of Directors are prohibited from: taking for themselves any business or investment opportunities that are discovered through or enhanced by the use of corporate property, information or position; using corporate property, information or position for personal gain; or competing with Consulate.

## BRIBERY AND CORRUPTION

***Integrity Inquiry: Are you or our agents putting yourself and the Company at risk by providing bribes, kickbacks or inappropriate special favors to government employees, agents or customers to procure or retain business?***

This policy addresses bribery, corruption and kickbacks related to dealings with governmental officials, agents, vendors and customers.

### A. Bribery of Governmental Officials and Agents

Consulate develops and maintains good relationships and effective communications at all levels of government having authority over the areas in which the Company does business. Contacts with governmental officials, both in this country and abroad, whether direct or indirect, must be maintained as proper business relationships. These contacts must never suggest a compromise of the objectivity of such persons or cast doubt on the Company's integrity.

U.S. laws, such as the Foreign Corrupt Practices Act (FCPA), many international laws, and Consulate policy, require accurate books and records, including those for payment of fees and gratuities. The FCPA and other laws make it illegal to pay, authorize, promise or offer a "corrupt" payment (or anything of value) directly or indirectly to a foreign government official, candidates for public office, agents, or relatives of that official for the purpose of causing the foreign government official to act or fail to act or otherwise use his or her influence to assist Consulate in obtaining, retaining or directing business.

A "corrupt payment" is one that intends to influence the recipient, or ultimate recipient, to misuse his official capacity to direct business, whether or not it has that effect. An employee of a government-owned enterprise may also be a "foreign government official" under the FCPA as may employees of organizations such as the International Monetary Fund ("IMF"). There are significant monetary fines for Consulate and potential imprisonment for individual employees for violation of the FCPA.



 

Bribery is also illegal in every country in which we do business, and most of those countries do not permit the "facilitating" or grease payments, which are permitted in limited circumstances under the FCPA, such as obtaining permits, licenses, or other official documents to qualify an entity to do business; processing governmental papers, such as visas and work orders; providing police protection, mail pick-up and delivery; scheduling inspections associated with contract performance or transit of goods across country; providing phone service, power and water supply, loading and unloading cargo, or protecting perishable products; and other actions of a similar nature. These payments are required to be accurately recorded in our books and records.

Even if you think a payment is allowable under the FCPA, you are required to have the approval of the country VP/Managing Director **and** either the VP, Global Compliance and Business Standards at 1-800-62-CONSULATE or an attorney in Consulate's Law Department before making what you think is a permissible payment or before Consulate (1) hires any foreign agent, representative or consultant or (2) enters into a joint venture agreement with an international party so that appropriate due diligence can be conducted.

The Company will provide training and require annual certifications from certain employees. Compliance with the FCPA is also mandatory for our agents. For more information on this policy, consult the International Compliance Manual located on the intranet.

**FREQUENTLY ASKED QUESTIONS:**

**Q:** *I know that Consulate is trying to expand internationally and that in some countries you have to pay or "take care of" an official or an agent to obtain valuable contracts. If there is no law that explicitly prohibits these payoffs in the other country, are we allowed to make the payments to get the business? I have heard that other companies do it all the time. If we don't make the payments, we can't be competitive.*

**A:** The Foreign Corrupt Practices Act prohibits such payments, even if it is a local practice or custom in the other country. Although there may be some instance in which limited or "facilitating" payments may be permitted, you are not authorized to make such payments without the approval of the VP/Managing Director (of the Country/Region involved) and Global Compliance Group or the Consulate Law Department. Further, those payments must be accurately recorded in our financial books and records. Certain employees will be required to sign an annual FCPA compliance certification.

**Q:** *How do I know that the payment I have been asked to make may violate the anti-bribery laws?*

**A:** Possible red flags include:

- The country has a history of widespread corruption, bribery or FCPA violations;
- The industry that you are dealing with has a history of FCPA violations;
- The agent refuses to certify that he or she will abide by the FCPA;
- An agent has family or business ties to a government official;

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

 

- An agent insists that his or her identity not be disclosed;
- A potential foreign government customer recommends a particular agent;
- An agent lacks the staff or the resources to perform the services;
- Local law forbids the agent to act as an agent;
- The agent makes statements that a particular amount of money is needed to get the business or "make the necessary arrangements";
- The payment or commission requested by the agent is substantially above the market rate, or the agent asks for a substantial up-front payment; or
- The agent requests payment by indirect means or in cash; requests false invoices or documentation; or requests that payment be made in a third country.

## B. Commercial Bribery/Kickbacks

In addition to bribery of foreign government officials, Consulate also prohibits commercial bribery, which refers to the practice of giving something of value to an intermediary (i.e., a customer's employee) without his/her supervisor's knowledge but with the intent of influencing the customer's commercial conduct. Consulate prohibits employees from providing or taking anything of value to gain an improper advantage in any transaction with actual or potential customers, vendors or suppliers.

### POLITICAL CONTRIBUTIONS

Employees may not make political contributions on the Company's behalf without the written approval of the General Counsel. This is not meant to prevent you from making personal contributions to the candidate of your choice. The Company will not reimburse you for any personal political contribution.

### GOVERNMENT CONTRACTS: INTEGRITY & ETHICS IN OUR BUSINESS

***Integrity Inquiry: Doing business with the government is not the same as doing business with commercial customers. Have you familiarized yourself with the rules?***

The government contracts industry is highly regulated. The rules are often complicated and not easy to understand. Regardless of what job you do, there are legal, regulatory and ethical standards that must be considered and upheld. You must strive to be aware of and understand the national, state and local laws—as well as the business requirements and practices—that affect your day-to-day duties, your department's operation and your area of responsibility. Failure to comply with the rules may result in disciplinary action or termination of employment, as well as potential civil and criminal penalties for you and the Company. It is, therefore, in your best interest to know and comply with the Company's legal



 

obligations. This section is a summary of some of the key regulations. More detail is available in the Company's Government Contracting Manual.

## PROCUREMENT INTEGRITY LAWS

The Procurement Integrity Act protects the process by which federal agencies acquire goods or services by using competitive procedures to award contracts. The Company will strictly adhere to the requirements of the Procurement Integrity Act, which applies to procurement competitions for contracts in excess of $100,000. Substantial civil and criminal penalties will apply to both the Company and any of our employees who violate the Act.

Under the Act, Company employees may not receive "source selection information" from current or former government officials who attempt to improperly influence the bidding process. Such information includes:

- Bid prices for sealed bids or lists or prices
- Source Selection plans
- Technical evaluation plans
- Technical evaluations of competing proposals
- Competitive range determinations
- Rankings of bids, proposals or competitors
- Cost or price evaluations
- Source Selection Board reports and evaluations
- Source Selection Advisory Board recommendations
- Proposed costs or prices submitted
- Any other information marked as "Source Selection Information"

Also under the Act, Company employees may not improperly obtain contractor bid and proposal information – that is, non-public information submitted to a federal agency as part of or in connection with a bid or proposal. Such information includes:

- Cost or pricing data
- Indirect costs and direct labor rates
- Information about manufacturing processes, operations and techniques when marked "proprietary" or "source selection information" in accordance with the law or regulation
- Information marked as "contractor bid or proposal information"
- Any other material or information related to a specific procurement which a company making a bid deems proprietary

Once awarded, all contracts must be performed in compliance with specifications, requirements and clauses.



 

## CONTRACT NEGOTIATION LAWS

The Company is committed to competing fairly and ethically for business opportunities. Employees involved in the negotiation of contracts must ensure that all statements, communications and representations of fact to client representatives are accurate and truthful. No employee shall submit any claims, bids, proposals or any other documents of any kind that are false, fictitious or fraudulent.

As a company that works with the government, the Company is frequently required to provide cost or pricing data, together with a certification that such data are current, accurate and complete. Finance personnel will ensure that employees involved in the negotiations are familiar with this policy and the requirements of the Truth in Negotiations Act.

## CONFLICT OF INTEREST LAWS – GOVERNMENT EMPLOYEES

Federal law restricts the hiring of certain government employees who are currently or who have been involved in awarding or administering contracts to the Company. It is important to get advice from Global Compliance and Human Resources before recruiting, interviewing, hiring or assigning work to former U.S. Government employees. If a U.S. government official initiates any employment discussions, employees should immediately contact the Company's Vice President, Global Compliance and Business Standards at 800-62-CONSULATE or ethics@Consulate.com.

## ORGANIZATIONAL CONFLICTS OF INTEREST

Regulations governing government procurements limit the ability of a company or individual to compete or participate in a procurement if an organizational conflict of interest exists. These regulations exist (1) to ensure that government contractors do not gain an unfair competitive advantage due to other work done for the government and (2) to ensure that other work performed by a contractor does not cloud the contractor's objectivity in providing impartial advice to the government. Other circumstances can also create organizational conflicts of interest, so it is important that employees communicate with the VP, Global Compliance and Business Standards or the General Counsel whenever a potential conflict arises.

For further guidance and information on organizational conflicts of interest, please consult the Conflicts of Interest Policy.



 

# TRADE RESTRICTIONS AND EXPORT CONTROLS

***Integrity Inquiry: Are you keeping up with the restrictions on doing business internationally? Are you taking shortcuts or bypassing Company rules or the law so that you can get business done more quickly or because "everyone else does it"?***

The United Nations, the European Union, and a number of other jurisdictions impose certain restrictions or prohibitions on export and trade dealings with certain countries, individuals, and organizations. Although the list is subject to change and there are different levels of restrictions, current restrictions exist related to the Balkans, Belarus, Burma (Myanmar), Cote d'Ivoire (Ivory Coast), Cuba, Democratic Republic of the Congo, Iran, Iraq, Liberia, North Korea, Sudan, Syria, and Zimbabwe, Specially Designated Nationals ("SDNs"), narcotics traffickers and terrorist organizations. Contact the Global Compliance Group for updated listings or check http://www.treas.gov/offices/enforcement/ofac/programs if necessary. The Bureau of Industry and Security ("BIS") maintains additional "prohibited parties' lists" that the Company may need to consult in certain circumstances. For more information on this policy, consult the International Trade Compliance Manual on the intranet.

An export does not only include physical or tangible goods. Exports also include the transfer or services of technology to a citizen of another country via email, discussions (wherever they take place) and visits to any company facility. The controls also impose licensing requirements for export of certain products, services or technology. The restrictions or controls may include bans on:

- Exports to a sanctioned country;
- Shipments through a non-sanctioned country to a sanctioned country or vice-versa;
- Imports from or dealing in property originating in a sanctioned country;
- Travel to or from a sanctioned country;
- New investments in a sanctioned country; or
- Financial dealings involving a sanctioned country or designated individuals or entities.

## U.S. ANTI-BOYCOTT ACT

Consulate is required under federal law to report to the government, and to refuse to cooperate with any request concerning boycotts or related restrictive trade practices. Employees are prohibited from taking any action, providing any information, or making any statements that could be viewed as participation in an illegal foreign boycott. The penalties for violation of this law are severe. Although the list is subject to change, currently the U.S. government has indicated that the following countries may require participation in a prohibited international boycott: Kuwait, Lebanon, Libya, Qatar, Republic of Yemen, Saudi Arabia, Syria and United Arab Emirates. There may be language in contracts regarding doing business with certain countries, ethnic, racial, religious or gender groups; these contracts must be analyzed carefully to ensure that compliance with the contract does not violate U.S. law.



 

You must immediately notify the Global Compliance Group, either orally or in writing, if you receive boycott-related requests. The Company may be required to notify the U.S. Government. For more information on this issue, please refer to the International Trade Compliance Manual located on the intranet.

## ANTI-MONEY LAUNDERING AND OFAC POLICY

Money laundering is a crime. It involves the movement of money from illegal sources or unlawful activities into legitimate businesses or activities. It is also a crime to take money from legitimate sources and use it for unlawful purposes, such as providing funds to terrorists. Consulate has adopted this policy to protect the Company and its employees against any involvement in money laundering activities.

OFAC (the Office of Foreign Assets Control) is an office of the United States Treasury Department that maintains and publishes a list of countries, individuals and entities that are known or suspected terrorists or threats to national security. Consulate has a legal obligation to not do business with these persons and entities; to freeze all property and block payment of funds to anyone on the list; and to file timely reports of all such actions with OFAC. The sanctions are severe.

The Company will conduct its business in compliance with the following general principles:

- Verify the identity of our customers and maintain records of such verifications of identity, as required by law;
- Compare the names of customers, business associates, and payees with the OFAC list and process any matches as required by law;
- Refuse to accept funds from or to do business with customers whose money, the Company believes, is derived from criminal activity or from a sanctioned source;
- Train employees to identify red flag activities and report them to their manager or as directed in the anti-money laundering procedures for their business unit;
- The Company's Vice President, Global Compliance and Business Standards or the appropriate designate will review any suspicious activity and determine appropriate measures to be taken, consistent with applicable law. Examples would include refusing to open an account or rent a vehicle, severing relations with the customer or vendor, closing or freezing accounts and, when appropriate, filing the appropriate OFAC report or suspicious activity report ("SAR"); and
- Conduct periodic independent, internal audits to evaluate the effectiveness of the Company's anti-money laundering and OFAC policies and procedures.



 

# CONFIDENTIAL/PROPRIETARY INFORMATION

***Integrity Inquiry: Are you violating Company policy and possibly the law by giving confidential information to others, including customers, without making sure that it is authorized?***

All Consulate records and information relating to Consulate or its customers are confidential, and you must treat them accordingly. Employees who knowingly or unknowingly reveal information of a confidential nature are subject to immediate and appropriate discipline, up to and including termination, and when appropriate, legal action.

Confidential and proprietary information includes, but is not limited to Consulate's and its customers': intellectual property; trade and business secrets; best practices; customer requirements; copyrights; patents; logos; trademarks; employee data; software code and modifications; customer, vendor and supplier lists; computer-generated reports; electronic information and software stored and used on computers; data used in the course of business; electronic mail; costs; profit and loss statements and financial data; markets; plans for future development; corporate strategy; contracts with other parties; product lines and products; bids and quotes; pricing information, and other business information not available to the public.

## REMOVAL FROM PREMISES

You may not remove any Consulate or Consulate-related information from Company premises (except in the ordinary course of performing duties on behalf of Consulate while employed by Consulate) without approval from an individual at director level or above. Such information includes, without limitation: documents, notes, files, records, price lists, manuals, employee data, computer files or similar materials as listed above.

## DISCLOSURE

When the Company entrusts you with its confidential or proprietary information, you must not use this information except in the performance of your duties as a Consulate employee. You may not disclose any confidential or proprietary information, purposefully or inadvertently (i.e., through casual conversation in an elevator or on an airplane) to any unauthorized person inside or outside of the Company.

Both during and after your employment with the Company you may not disclose, copy, sell or distribute confidential and proprietary information to: any third party or any other Consulate employee (unless it is on a "need to know" basis). You may not copy, replicate or load any confidential and proprietary information onto any computer (including your home computer), other than a computer provided to you by Consulate, without permission from your manager.

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

You are also responsible for keeping confidential information in a secure location and not leaving copies of such information in unsecured areas, and at Consulate's request, immediately returning all confidential and proprietary information, including notes, records, documents, diskettes, computer data, etc.

If you are unsure about the confidential or proprietary nature of any specific information, ask your supervisor or the Global Compliance Group for clarification.

**FREQUENTLY ASKED QUESTIONS:**

**Q:** *A few of my family members work in our industry for other companies, who are not competitors of Consulate. At family gatherings, we eventually start "talking shop." Why would this be a problem?*

**A:** Unfortunately, conversations about the industry or Consulate in particular may lead you to reveal confidential information to your relatives. Unless the information is publicly available, you must avoid discussing it. Discussions of industry issues might not only violate the Company's confidentiality policy, but could violate antitrust laws as well, depending on the topics discussed. Antitrust issues will be discussed separately in these Principles.

**Q:** *I often receive subpoenas and requests for information from the government or lawyers about my employees. Since the documents look like authentic legal documents, can I provide the information?*

**A:** All subpoenas and requests for information about our employees from the government, courts or non-Consulate attorneys must be forwarded immediately to the Law Department for handling.

## BLOGGING POLICY

In general, the Company views websites, web logs and other information published on the Internet by its employees positively, and it respects the right of employees to use them as a medium of self-expression. If you choose to identify yourself as a Consulate employee or to discuss matters related to our business on the Internet, please bear in mind that although the information you publish on the Internet will generally be viewed as a medium of personal expression, some readers may nonetheless view you as a de facto spokesperson for the Company. In light of this possibility, we ask that you observe the following guidelines:

- Make it clear to your readers that the views expressed are yours alone and do not necessarily reflect the views of the Company.
- Understand that you assume full responsibility and liability for your public statements.
- Do not disclose any information that is confidential or proprietary. For example, projected revenue or profits, customer details, or product and service developments that have not been made public, should not be discussed. Always err on the side of caution by reviewing Consulate's policy on confidential and proprietary information.
- The Company requires that you seek permission before using its trademarks on your publications on the Internet.

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

 

Since the information you publish on the Internet is accessible by the general public, the Company expects your comments will be truthful and respectful to the Company, its employees, customers, partners, affiliates and others (including our competitors) as the Company itself endeavors to be. If you are going to criticize individual employees, consider discussing the criticism personally before making it public. The Company will not tolerate statements about the Company or its employees that are defamatory, obscene, threatening or harassing.

Please be aware that the Company may request, in its sole and absolute discretion, that you temporarily confine your website, web log or other Internet commentary to topics unrelated to the Company if it believes this is necessary or advisable to ensure compliance with securities regulations or other laws.

Failure to comply with these requests may lead to discipline up to and including termination, and if appropriate, the Company will pursue all available legal remedies.

Consult the Company's E-Mail, Internet, and Voice Mail Policy for additional information.

If you need clarification of any aspect of this policy, contact your supervisor or the Global Compliance Group.

**Note: By publishing these guidelines, the Company is not assuming a duty to monitor Internet activity but reserves the right to take appropriate action in accordance with these guidelines in its sole and absolute discretion.**



 

# DATA PRIVACY: CONFIDENTIAL INFORMATION OF EMPLOYEES AND OTHERS

***Integrity Inquiry: Are you doing everything you can to protect Company, customer and employee information from theft or unauthorized access or disclosure? Do you know what to do if there is a data breach?***

Consulate collects and processes data for a variety of business-related purposes. On occasion, some of the information may constitute personal data that can be used directly or indirectly to identify a living individual and may include sensitive categories of information. The Company is committed to complying with the applicable privacy and data protection laws in the countries in which we operate. If you have questions regarding these policies, contact the Chief Privacy Officer at ethics@Consulate.com.

Sensitive information may include religion, political opinions, health condition, financial statements, racial or ethnic origin, date of birth, identity card numbers, marital status, occupation, income, and other information.

Your obligations as an employee or manager include, but are not limited to, the following:

- Documents or computers that contain employee Social Security/Social Insurance numbers must be securely locked or otherwise made private before leaving them unattended. Hit Control + Alt + Delete and then click on Lock Computer to safeguard the data when stepping away from your workstation.
- When outside of the Consulate work environment, including at airports, hotels or restaurants, do not leave your laptop unattended for even the shortest period of time. Never leave your laptop unattended in any vehicle.
- Complete or partial Social Security/Social Insurance numbers must not appear on any documents other than those absolutely required for benefits, payroll or profile processing. Do not use these numbers on disciplinary forms, performance appraisals and other documents.
- Treat documents or other records containing credit card or debit card numbers, bank account or other financial information, medical/health information, drivers license numbers and any other sensitive personal information the same way you treat documents with Social Security/Social Insurance numbers.
- Documents containing sensitive personal information must be safeguarded by properly and appropriately securing them and not leaving them unattended where an unauthorized employee, customer or third party could have access.
- Ensure that laptops, Blackberries, PDAs and other portable media have additional security measures, such as password protection, encryption or other mechanisms so that confidential data is inaccessible to others.

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

- Allow customers and employees to review their personally identifiable data and to correct it, when necessary. If you are unsure or in any way uncomfortable about providing access to the information, please contact the Chief Privacy Officer.
- Do not send mass faxes or emails to potential customers without their written or expressed permission, and without providing an opportunity for them to opt out of the communication. When in doubt, contact the Chief Privacy Officer or the Law Department.
- Always securely lock up any document or file that has an employee's or customer's Social Security/Social Insurance number, driver's license number, credit card or debit card number, medical/health information or other personally identifiable and confidential information. When appropriate, and in accordance with your department's document retention requirements, disposed files and documents should be shredded. Electronic files (or the personal information contained in such files) must be made rendered unreadable. Contact IT or the Chief Privacy Officer if you have any questions regarding disposal of these kinds of files. Discarding the document in a garbage can or dumpster without shredding it or otherwise making the information unrecognizable is a violation of Company policy, and in some cases, the law.
- Report any actual or suspected break-in at a facility or theft of a laptop, computer, storage media or documents that may contain employee or customer data to Global Security and the Chief Privacy Officer immediately, even if you do not know what information may have been accessed. There are laws that may require notification to those whose information may have been compromised.

In order to comply with this policy and ensure maximum protection for the employee and customer data, please password protect sensitive documents with the types of information described above. Please note: You should carefully track the password used on a document as these passwords are not recoverable. For shared documents, choose a password common to both users of the document in order to not share personal information.

**Failure to comply with this policy may lead to disciplinary action, up to and including termination.**

For assistance protecting documents, contact Consulate IT. For more information on global privacy issues, please contact the Chief Privacy Officer or the Global Compliance Group at ethics@Consulate.com.

**FREQUENTLY ASKED QUESTIONS:**

**Q:** *My car was broken into and I had some work-related files in it. What do I need to do?*

**A:** Immediately contact the Chief Privacy Officer at ethics@Consulate.com and Global Security. Depending on the kind of information that may have been stolen, we may have a legal obligation to inform customers or employees about the theft. There may be strict fines and penalties for failure to provide the notification in a timely manner.

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

 

## COMPETITIVE INFORMATION/COMPETITIVE INTELLIGENCE POLICY

To be a successful competitor in today's environment, Consulate needs accurate and detailed information about the markets in which it competes and the activities of its rivals. Indeed, most companies gather competitive information on their competitors to stay abreast of "best practices" in areas such as product development, marketing and sales, and operations.

The antitrust laws do not penalize a company for possessing competitive information. On the contrary, markets are typically driven by competitors knowing what their rivals are doing, which enables effective competitive responses.

However, the antitrust laws do make the acquisition of competitive information from certain sources very risky. The Company has developed guidelines, which are available on the intranet or through your management, to help you assess the legal risks posed by the use of various methods of gathering competitive information. These guidelines should be consulted whenever you contemplate, among other things, (i) any informal exchange of competitive information, (ii) conducting a competitive analysis or survey, or (iii) participating in a survey conducted by a competitor or non-competitor third party. When in doubt, you should seek advice from Global Compliance or any member of Consulate's Law Department before participating in any exchange of competitive information, or conducting or participating in any competitive survey. You should also refer to the Antitrust Policy, described in these Principles, and also available on the intranet.

## WORK PRODUCT OWNERSHIP

Consulate retains legal ownership of the work product of all full-time employees, part-time employees, temporary workers and independent contractors.

Work product includes: written and electronic documents, audio and video recordings, system code, and any concepts, ideas or other intellectual property developed for Consulate, regardless of whether the intellectual property is actually used by the Company. No work product created while you are employed or contracted by Consulate can be claimed, construed or presented as your property, even after your employment with the Company is terminated or the relevant project completed.

If appropriate, the Company may take civil and/or criminal action against anyone violating this policy, and will seek repayment of all legal fees and costs.

Supplying other entities with certain work product or elements of work product may constitute a conflict of interest. In some situations, such as on a resume or in a freelancer's meeting with a prospective client, you may display and/or discuss a portion or the whole of certain work product. However, to avoid a conflict of interest, you must ensure that any information classified as confidential remains so, even after your employment or contract with Consulate has ended.



 

# COMPUTER SECURITY AND CONFIDENTIALITY/USE OF COMPANY COMPUTERS

All software and data resident on all Company computers (e.g., mainframe, workstation or portable computers), whether in production or being tested by the Company, are the sole and exclusive property of Consulate.

As an employee of Consulate, you are responsible for taking all appropriate actions, whether by instruction, agreement or otherwise, to ensure the protection, confidentiality and security of confidential information.

Written authorization from a director-level manager is required before you may acquire, use, access, copy, remove, modify, alter or disclose to any third parties, any confidential information for any purpose other than to perform duties required in fulfillment of your job responsibilities or in furtherance of expressly stated Company-sponsored activities.

## IDENTIFICATION AND PASSWORD

You are responsible for all activity performed with the use of your identification or password. Upon request, you must provide Consulate management with any passwords for access to systems, documents or any other work product created during your employment with Consulate or created on Consulate-owned hardware or with Consulate-owned software. You may not share your passwords with other employees unless you are required to do so by your manager for a specific project or other work-related purposes. You are responsible for changing your password and protecting it upon completion of the project.

## ASSIGNED COMPUTERS

You are responsible for protecting any Company-owned or provided computer to ensure that its data, software and hardware are not misused, and protecting and backing up your computer data.

## REPORTING BREACHES IN SECURITY

If you become aware of any breach in security you should immediately report it to your supervisor. If the security breach involves customer or employee information, you must immediately contact the Company's Chief Privacy Officer at 1-800-62- CONSULATE or **ethics@Consulate.com** and Global Security.

## TERMINATED EMPLOYEES

When you terminate employment with the Company whether voluntarily or not, you must immediately return all Consulate-related information, equipment and property in your possession.

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

**FREQUENTLY ASKED QUESTIONS:**

**Q:** *I have some personal information on my computer that I work on during my breaks or after hours. I also get personal emails. Does my manager have the right to read my personal documents? What about my privacy rights?*

**A:** Unless otherwise prohibited by law, Consulate managers have the right to review any items on the Company's computer, email, or voicemail systems, without notice to or consent from you. The Company also has the right to examine your Internet access if you use Consulate's computers, including laptops. Some incidental use of computers for personal use is generally permitted if approved by your manager and you comply with the Company's standards as outlined in the Employee Handbook, the Policy Against Harassment, Discrimination and Retaliation ("HDR") and other policies. However, you must remember that Consulate's systems belong to the Company and are primarily for work-related purposes. You are never permitted to have material that is defamatory, obscene, racist or otherwise violative of Company policies, even if you do not display it to others. Having these materials on your computer will subject you to disciplinary action, up to and including termination.

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

 

# ENVIRONMENTAL POLICY

***Integrity Inquiry: Can you identify your Environmental Coordinator? Are you staying informed of the Company's environmental policies and programs?***

Consulate is committed to supporting the important goals of sustainable development, environmental protection, and pollution prevention in its business of providing transportation and logistics solutions around the world.

Toward this objective, Consulate is dedicated to developing and implementing effective environmental practices in all of its business activities, and to continually monitoring these practices to identify opportunities for improvement. Consulate's environmental leadership team works with all levels of staff and operating employees to develop and administer programs in support of the Company's environmental policy. Employees have a responsibility to stay informed about environmental policies and programs and to take immediate corrective action to address any adverse situation or condition.

Each Consulate facility has a designated Environmental Coordinator responsible for overall environmental compliance. Employees must know who their Environmental Coordinator is and how to reach him/her if needed. Consulate communicates the Company's established environmental policies and its programs in support of these policies to all locations. Policies are also located on Consulate's Intranet site.

You are required to read and understand all environmental policies and procedures, perform job responsibilities consistent with established policies, and report all deviations and/or non-compliance with environmental policies to your supervisor and Consulate's Environmental Services Group.

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

# ANTITRUST POLICY

***Integrity Inquiry: Are you talking to competitors about price, confidential information, allocating territories or customers or customer boycotts? There are almost no circumstances in which such conduct is allowed.***

Consulate and its employees will strictly comply with both the letter and the spirit of the antitrust laws in all of the jurisdictions in which we do business. Employees must avoid any activities that violate, or even appear to violate, antitrust laws. There is no exception to this policy. Any violation of Consulate's Antitrust Policy will be cause for disciplinary action, up to and including termination. See the Competitive Intelligence Section for additional guidance on antitrust issues.

## KNOWLEDGE OF LITIGATION

If you become aware that antitrust litigation has begun or has been threatened against Consulate, a competitor, a customer or a supplier, promptly notify the Consulate Law Department or the Global Compliance Group. This notification is necessary, even if it appears to you that the Company is not involved.

## DISCLOSING OR RECEIVING PRICE INFORMATION FROM COMPETITORS

Consulate's prices are to be arrived at independently. Never discuss prices or pricing policy with a competitor, give a price list or pricing information to a competitor, exchange a price list or pricing information with a competitor, or exchange such information through a third party.

Any agreement with a competitor concerning prices other than a legitimate buy-sell relationship is per se illegal, that is, without regard to what the agreeing parties intended and without the need to provide actual injury to competition. There is no defense, justification, or excuse of any kind for such agreements. The act of agreeing in and of itself, even if the agreement is not successfully implemented, is illegal. An agreement may be inferred from your actions. Neither a written document nor a handshake is necessary for an illegal agreement to exist. Responding to pressure or doing what you know is expected by a competitor can be sufficient. Therefore, avoid contacts with competitors that may raise suspicions that an agreement may exist.

It is illegal to agree with a competitor on a formula for computing prices, price differentials, or minimum or maximum prices. It does not matter that the price agreement is one in which the prices are decreased rather than increased; prices are stabilized; agreed upon prices are reasonable; prices agreed upon are not uniform, or; purpose of the agreement is to prevent ruinous competition. Agreeing to elements of price and to terms and conditions of sale (e.g., discounts, freight charges or credit) can be found to be just as illegal as agreeing to price itself.



 

The only exceptions to these rules are for a communication of price in connection with a bona fide sale to, or purchase from, a competitor, and discussions limited to labor rates and benefits for informational purposes in connection with multiple-employer collective bargaining.

**Important:** Be sure to note the date and source of all price information obtained from customers on the face of the material received.

## ALLOCATION OF TERRITORIES

It is illegal for competitors to divide or allocate territories in which they will sell. The only exception may be a non-compete agreement in connection with the purchase of a business from a competitor. Never agree with a competitor to sell or refrain from selling in any area.

## ALLOCATION OF CUSTOMERS

It is illegal for competitors to divide or allocate the customers to whom they will sell. Never agree with a competitor to sell or refrain from selling to any customers or class of customers, and never agree to divide or share a customer's or potential customer's business with a competitor.

## AGREEMENTS TO RESTRICT OR STANDARDIZE SERVICES

It is illegal for competitors to enter into an agreement to restrict or increase the availability of products or services. In many cases, an agreement among competitors to standardize services or equipment may be illegal. Sometimes standard-setting organizations or customers will attempt to establish industry standards. If you believe there is a valid business reason for such an agreement, contact the Consulate Law Department or the Global Compliance Group before you have your first discussion on this subject with a competitor.

## BOYCOTTS AND REFUSALS TO DEAL

It is illegal to enter into an agreement with competitors not to sell to or buy from certain individuals or firms. Never suggest that a competitor not sell to or buy from any particular source. As a general rule, you have a legal right to choose your suppliers and customers and to refuse to buy from or sell to anyone. But, this right must be exercised independently, without consultation from outside the Company.

## DEALINGS WITH CUSTOMERS AND SUPPLIERS

A supplier or manufacturer may impose minimum resale prices and territorial or customer restrictions on a distributor or retailer and refuse to sell to a distributor or retailer that discounts goods below suggested prices or sells outside of its assigned territory or customers. Although it is not per se illegal, there is a risk involved in agreeing with manufacturers, suppliers, distributors or retailers to set the minimum price at which a product may be resold, or agreeing to territorial or customer restrictions. Courts will examine these transactions carefully. Contact the Law Department or the Global Compliance Group before agreeing to minimum resale prices or territorial or customer restrictions.

Moreover, it may be illegal to sell a product or service only on the condition that the customer purchases another product or service from Consulate. Do not force a customer to purchase an additional type of



 

product or service not desired by that customer in order to get a desired product or service from Consulate.

It may be illegal to sell or lease on the condition that the purchaser or lessee not deal with a competitor. It may also be illegal for a buyer to purchase goods or services only on the condition that the seller purchases the buyer's products. In essence, this is an agreement in which, "I'll buy from you only if you buy from me." Consulate's purchases and sales should be solely on the basis of price, quality, terms and service. Never tell customers that you will do business with them only if they agree to purchase or lease from Consulate. Never tell customers that they should purchase or lease from Consulate because Consulate purchases from their organizations.

This does not mean that a Consulate customer cannot supply Consulate, but it does mean that Consulate's decision to use a supplier must be independent of the supplier's decision to use Consulate. Each employee, officer and director should endeavor to deal fairly with Consulate's customers, suppliers, competitors and employees. No one should take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair-dealing practices.

## PRICE DISCRIMINATION

Consulate cannot use its size or purchasing power to extract an unlawful advantage from its suppliers nor can it treat competing customers differently. It may be unlawful to sell the same product to competing customers at different prices. Do not insist on volume discounts, rebates, or allowances from a supplier when they are not similarly offered by the supplier to its other customers.

## UNFAIR METHODS OF COMPETITION

To avoid the appearance of unfair methods of competition do not sell at unreasonably low prices or below cost for the purpose of eliminating competition or a competitor, and do not tell a supplier to refuse to deal with a competitor.

## TRADE ASSOCIATIONS

If you are involved with a trade association, you must be particularly alert to Consulate's policy of strict compliance with the letter and spirit of the antitrust laws. Trade associations provide a number of useful services and activities for their members. However, they merit special and careful attention because they often provide opportunities for communications among competitors.

Consulate employees should not participate in, or even remain present at any discussion among competitors at an association meeting or other gathering of association members or participants if the discussion concerns prices or factors determining prices, delivery terms, allocation of territories among competitors, allocation of customers among competitors, and/or refusals to deal with customers or suppliers.

If you become aware of such a discussion, you must immediately ask that the discussion be stopped, request that the minutes of the meeting show your request, leave the discussion, and contact the Consulate Law Department immediately so that appropriate action can be taken.



 

## PENALTIES

Penalties for antitrust violations are severe for both the corporation and its employees. Litigation is extraordinarily expensive in terms of both dollars and time.

## REQUESTS FOR DOCUMENTS/INFORMATION

Consulate will cooperate with the various government agencies and departments. However, Consulate is entitled to all the safeguards provided by law. Therefore, never give any documents or information to a government employee or outside attorney without first contacting and receiving authorization from the Consulate Law Department.

## APPEARANCES

Avoid any conduct that could appear to constitute a violation of the law. No matter how innocent a particular act may be, legal difficulties can result if it leads others to believe that a violation has occurred.

**You may have close friends who work for competitors, customers, or suppliers. The Company is not asking you to give up these relationships. However, a mutual understanding that there will never be any improper discussion of business matters can avoid problems.**

### FREQUENTLY ASKED QUESTIONS:

**Q:** *I will be attending a large trade show next month and I know that some of our competitors will be there as well. Usually at these meetings, there is talk of the state of the industry and where people expect pricing to go. Participating in these conversations is very helpful to me and to Consulate. Why would this be a problem?*

**A:** You should use extreme caution in these situations and not discuss the pricing or terms of any Consulate contracts. Nor should you attempt to gain competitive information directly from a competitor. You should refuse to discuss any anti-competitive issues, leave such conversations immediately and promptly disclose the issue to the Global Compliance Group.

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

 

# DOCUMENT RETENTION AND DESTRUCTION POLICY

***Integrity Inquiry: Are you keeping any documents, emails or other media longer than required by law or Company policy? Have you checked the Document Retention Manual to make sure you know the rules?***

The Company's Document Retention and Destruction Policy serves the information and record management needs of the business and ensures legal compliance. (The words "document" and "record" are used interchangeably in these guidelines.) Wrongful destruction, alteration or falsification of records may subject the persons involved and the Company to civil liability and criminal penalties. The full policy is located on the intranet, as are document-specific guidelines. While it is beyond the scope of this policy to list the detailed categories of information and retention periods covered by this policy, the following is provided as a general guideline:

- All records shall be retained for the period required by applicable state and federal laws and regulations.
- Adequate records shall be developed and maintained to document the Company's compliance with all relevant laws and regulations.
- All records necessary for business reasons shall be retained for a period of time that will reasonably assure the availability of those records when needed.
- Records vital to the ongoing operation of the business shall be identified and appropriately safeguarded.
- All records not necessary for legal or business reasons and not required to be retained by law or regulation shall be destroyed in order to reduce the high cost of storing, indexing, and handling the vast amount of documents that would otherwise accumulate and to maximize the performance of the computer systems.
- Destruction of records shall take place only in compliance with a standard written policy in order to avoid any inference that any document was destroyed in anticipation of a specific problem.

**Documents that are not otherwise subject to retention for business reasons may need to be retained because of unusual circumstances, such as litigation or a government investigation. If for any reasons one of these unusual circumstances exists or arises, the Law Department shall be notified immediately. When litigation or investigations occur, the Law Department will notify the appropriate departments and direct that relevant categories of documents be labeled for retention until further notice. This is also known as a "litigation hold." You may not destroy, alter or falsify any paper or electronic document (i.e., email, voicemail) or other record that may be relevant to an anticipated, threatened or pending lawsuit or investigation, whether internal or external.**



 

The privacy and security of records shall be appropriately assured.

This policy applies to records maintained on all types of storage media, including electronic and voice storage. With the increasing reliance on email and other electronic documents to conduct the Company's business, it is crucial to adhere to document retention procedures governing the preservation of electronically stored information upon anticipation of litigation or investigation.

Records, such as notes, memoranda, letters, reports, computer disks, tapes, and so forth, located in individual offices, at home, or any other offsite location are subject to these guidelines and shall be managed consistent with these guidelines.

Specific questions regarding the Company's document retention policy should be directed to the Global Compliance Group or any Consulate lawyer.

### EXCEPTIONS

Requests for exceptions to this policy must be submitted to the Global Compliance Group or the Law Department for approval before implementation. In order to obtain an exception to this policy, there must be a program that will assure compliance with the basic objectives stated above at least as effectively as this policy.

## REPORTING MECHANISM AND POLICY AGAINST RETALIATION

If you reasonably believe that a violation has occurred, you **must** report it immediately to your supervisor, human resources, any manager, the Global Compliance group at (800) 62-CONSULATE, or the Vice President of Audit Services at (305) 500-4255, and you may do so confidentially. You may make a confidential and anonymous report through the Consulate HOTLINE at (800) 815-2830, 24 hours a day, seven days a week, or by completing a report through Consulate.com. There are no tracking or tracing mechanisms, such as caller ID or other email identifiers. The reporting mechanisms are available to customers, suppliers, vendors, or anyone who has information about a suspected violation. **Consulate forbids retaliation against any employee who files a good faith report. If you believe that you have experienced retaliation, contact any manager, human resources or the Global Compliance Group.**

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

 

# ACKNOWLEDGMENT

## ACKNOWLEDGMENT OF RECEIPT OF THE CONSULATE PRINCIPLES OF BUSINESS CONDUCT

I acknowledge that I have received a copy of Consulate's Principles of Business Conduct. I agree to read it thoroughly and abide by the policies. If there is any policy or provision that I do not understand, I will seek clarification.

In addition, I understand that the Principles state Consulate's policies and practices in effect on the date of publication and that policies and procedures are continually evaluated and may be changed or eliminated at any time, with or without notice.

Name (Please Print): _____

Personnel/SAP Number: _____

Location: _____

Signature: _____

Date: _____

cc: Personnel File

***For guidance on compliance and ethics issues contact the Global Compliance Group through the ethics line at 1-800-62-CONSULATE or ethics@Consulate.com. To file a report with an independent third party, contact the Hotline at 1-800-815-2830.***

# Foreign Corrupt Practices Act ("FCPA") Certification

1. I _____currently serve as _____ in Consulate's operation located in _____.

2. I have received and read Consulate's policy statement on Gifts, Meals, Entertainment, Travel and Charitable Contributions, including the list of "red flags," which is attached to this Certification. I understand that I am required to abide by the Foreign Corrupt Practices Act ("FCPA") and any local laws regarding bribery.

3. The statements made in this certification are based upon knowledge and understanding of the FCPA as outlined in the attached policy.

4. Based upon my awareness and understanding of information referenced and set forth in paragraphs 2 and 3 above, and to the best of my knowledge, information and belief:

- I am not aware of any payment made, directly or indirectly, to or for the benefit of any foreign official for the purpose of obtaining or retaining business, except as reported in paragraph 5 below.

- I am not aware of any payment made, directly or indirectly, to or for the benefit of any foreign political party, official or candidate for the purpose of obtaining or retaining business, except as reported in paragraph 5 below.

- I am not aware of any payment made, directly or indirectly, to or by a third party or agent with knowledge that it would be offered to a foreign official, or foreign political party, official or candidate for the purpose of obtaining or retaining business, except as reported in paragraph 5 below.

- I am not aware of any payment made, directly or indirectly, to or for the benefit of any employee of a government-controlled business, corporation, company or society for the purpose of obtaining or retaining business, except as reported in paragraph 5 below.

- I am not aware of any entry recorded in any book, record or account that might be interpreted as misstating or concealing the nature or purpose of any payment or expenditure, except as reported in paragraph 5 below. I am not aware of the maintenance of any cash fund, "slush fund," bank deposit or other asset that is not recorded in the financial and accounting books and records, except as reported in paragraph 5 below.

- I have never participated in or assisted, nor do I have knowledge of, any conduct by any Consulate employee, partner or agent that, in my judgment, either does not comply with the FCPA or has the appearance of not complying with the FCPA, except as reported in paragraph 5 below.

- I am also unaware of any instances of commercial bribery, which involves providing or agreeing to provide anything of value to an intermediary (e.g., a customer's employee) in

 

order to gain improper advantage in the commercial setting with actual or potential customers, vendors or suppliers, except as reported in paragraph 5 below.

5. Exceptions to paragraph 4 are noted on a separate page attached to this Certification or have been or will be reported by me through one of the Company's various reporting mechanisms, including management, the Hotline, ethics@Consulate.com, or the Global Compliance and Business Standards office. I understand that I have an obligation to make a report, but that I may do so anonymously, and will keep a record of my report.

6. I further certify that all pending, future or renewed contracts or agreements for the retention of consultants, agents or representatives will be reviewed in advance by Global Compliance, and will generally contain the following:

    a. A requirement that the person will comply with all applicable laws and regulations, including the FCPA, in the course of all activities on the Company's behalf.
    b. A requirement that the consultant will file periodic reports with the Company regarding his or her activities on the Company's behalf.
    c. A requirement for an identification of all principals and subagents.
    d. A provision prohibiting the consultant from refunding any Company funds to any director, officer, employee or other agent of the Company or a customer or from making any illegal payment from the funds under applicable laws; and
    e. A provision which terminates the agreement without any further liability or obligation on the part of the Company should the consultant breach any of these covenants.

I certify to the statements described above.

_____
Name (print)

_____
Name (signature)

_____
Title

_____
Date

 

# PROPOSED REPRESENTATIVE QUESTIONNAIRE

The questionnaire on the following page must be completed by Consulate's distributors, consultants, joint-venture partners and other third party representatives (referred to as "Proposed Representatives"). Once it has been returned, it must be reviewed against the Representative Due Diligence Checklist.

## PROPOSED REPRESENTATIVE QUESTIONNAIRE

The following information will assist Consulate in assessing the qualifications of ("Proposed Representative") to act as a Representative to Consulate in the country of . Your cooperation in completing this form is important to Consulate and is greatly appreciated. Please attach additional sheets of paper as needed.

1. Name of Proposed Representative:

   Principal Contact:

   Address:

   Telephone:

   Fax:

   Email:

2. Year established:

3. Registration number:

4. Type of organization (sole proprietorship, partnership, corporation, etc.) and place of organization and/or registration:

5. Number of employees:

6. Please list the names and addresses of all officers, directors and owners of the Proposed Representative, together with the ownership percentages of all owners. (Owners holding less than a 5 % interest in the Proposed Representative may be omitted, unless they are officers or directors.)

| Name | Position(s) (officer, director, owner) | Ownership % |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

 

7. Please list all affiliated business enterprises, including a description of their businesses and the location of their principal place of business.

| Affiliated Enterprise | Description of Business | Location |
|---|---|---|
| | | |
| | | |
| | | |

8. Please describe Proposed Representative's current business activities (if a distributor or dealer, please include other products handled):

9. Has Proposed Representative, any of its affiliates identified in Question #7 above, or any officers, directors or owners of Proposed Representative or its affiliates been a defendant in any civil litigation, any arbitrations, or any criminal proceedings in the last five years?

☐ Yes ☐ No

Has Proposed Representative, any of its affiliates identified in Question #7 above, or any officers, directors or owners of any of those companies been the subject of a criminal investigation in the last five years?

☐ Yes ☐ No

If you answered Yes to either of the last two questions, please provide a detailed explanation.

10. Please provide the name(s) and position(s) of the person(s) who will be principally responsible for Proposed Representative's relationship with Consulate.

| Name | Position |
|---|---|
| | |
| | |
| | |

 

| | |
|---|---|
| | |

11. Please describe the experience and the business or professional relationships of the person(s) named in Question #10 above, and of the Proposed Representative generally, that relate to the Proposed Representative's ability to be of assistance to Consulate.

12. Do any of the following individuals hold any position with any government, any government agency, any public (governmental) hospital or other health care institution, any international organization, any enterprise owned in whole or in part by a government, or any political party?

- Any owner, officer, director, or employee of Proposed Representative.
- Any family member of any owner, officer, director, or employee of Proposed Representative.

☐ Yes ☐ No

If Yes, please identify all such individuals, their positions, and the corresponding governments, agencies, organizations, and/or parties.

| Name | Position in / Relationship to Proposed Representative | Position in Government / Agency / Organization / Party |
|---|---|---|
| | | |
| | | |
| | | |

13. If the Proposed Representative is a subsidiary of another corporation or other entity, please provide the same information requested in Items 6, 9, and 12 for the parent corporation or entity.

14. Please provide the names of at least two commercial enterprises with which you have worked previously, as well as the name of a person at each of these enterprises who is familiar with the work that you did with his or her employer.

Name of Enterprise:

Contact Person:

 

Position:

Address:

Telephone:

Email:

Name of Enterprise:

Contact Person:

Position:

Address:

Telephone:

Email:

15. Please provide a local banking reference.

Contact Person:

Position:

Company:

Address:

Telephone:

Email:

16. Attached to this questionnaire is a copy of the representations and warranties that will be included in any agreement between Proposed Representative and Consulate.

Will Proposed Representative be able to satisfactorily perform its responsibilities under its agreement with Consulate, and at all times act in a manner that is consistent with the representations and warranties in the attachment?

☐ Yes ☐ No

If No, please explain.

 

17. Certification: I certify that the information above is correct and complete.

Signature: _____ Date: _____

Name: _____

Position: _____

 

# PROPOSED REPRESENTATIVE DUE DILIGENCE CHECKLIST

Directions: **Section A** must be completed by the Country Manager or his/her designee with the assistance of Global Compliance and Global Security to perform the substantive due diligence and record searches. **Section B** must be completed by the Country or Regional Manager in consultation with Global Compliance.

## Section A: Due Diligence Review

1. Name of Proposed Representative:

2. Describe Proposed Representative's duties:

3. Attach a completed copy of the Proposed Representative Questionnaire, including information listing the names of all officers of the Proposed Representative and all owners of interests greater than five percent (include alternate spellings if the name is a transliteration from a language not written in the Roman alphabet).

4. Run the names of the Proposed Representative, its owners, and its officers (including any alternate spellings) through the Company's database which includes various terrorist watchlists as well as the names of Politically Exposed Persons. Search Google and Nexis or Westlaw database of newspapers and periodicals (including database of foreign language periodicals where relevant and possible). Review relevant websites and articles in newspapers and periodicals. Contact Global Compliance if additional resources are needed to perform this task. Do these materials indicate:

   a. that Proposed Representative or any of its officers or owners may have been involved in improper activity of any sort?

      Yes ☐ No ☐

      If Yes, provide details on a separate piece of paper.

   b. that Proposed Representative (if an individual) or any of its officers or owners holds any position with any government, any agency or

 

instrumentality of any government, any enterprise in which a government owns an interest, or any political party?

Yes ☐ No ☐

If Yes, provide details on a separate piece of paper.

c. that Proposed Representative (if an individual) or any of its officers or owners is now, or recently has been, a candidate for political office?

Yes ☐ No ☐

If Yes, provide details on a separate piece of paper.

5. Speak with the commercial and banking references provided by Proposed Representative, and any other commercial sources as you think appropriate. In these discussions, elicit information concerning the nature of the relationship between Proposed Representative and the reference. Also, ask specifically: (i) whether the reference has any reason to believe that the Proposed Representative would be anything other than completely honest in its business dealings, and (ii) whether the reference has any reason to believe that the Proposed Representative would violate a commitment not to bribe employees of governmental bodies.

a. Did all of the references recommend Proposed Representative without reservation?

Yes ☐ No ☐

If No, provide details on a separate piece of paper.

b. Do any of the references have reason to believe that the Proposed Representative would be anything other than completely honest in its business dealings?

Yes ☐ No ☐

If Yes, provide details on a separate piece of paper.

c. Do any of the references have reason to believe that the Proposed Representative would violate a commitment not to bribe employees of customers or governmental bodies?

Yes ☐ No ☐

If Yes, provide details on a separate piece of paper.

 

6. Speak with the Company employee(s) who initially suggested the Proposed Representative. (For renewals, only items f. and g. below are required.) Record their answers to the following questions:

   a. Are there any Company employees who are more familiar with the Proposed Representative's business and reputation?

      Yes ☐ No ☐

      If Yes, interview those employees in addition to the proposing employees and also obtain their answers to the following questions.

   b. Why does the Company need the Proposed Representative's services?

   c. How did the Proposed Representative first come to the Company's attention?

   d. Describe the Proposed Representative's relevant experience as well as the source(s) of this information.

   e. Describe the Proposed Representative's relevant contacts with customers and governmental regulatory bodies, if any, and the source(s) of this information.

   f. Why is it potentially advantageous to the Company to enter into an agreement with the Proposed Representative rather than other possible Representatives in the territory?

   g. Do the employees believe that the Proposed Representative would comply with a contractual commitment not to bribe government officials or employees?

      Yes ☐ No ☐

      If No, provide details on a separate sheet of paper.

 

h. Do the employees think it likely that the Proposed Representative has paid bribes in the past for any purpose?

Yes ☐ No ☐

If Yes, provide details on a separate sheet of paper.

7. If available, request and attach a standard Proposed Representative Investigation Report from an outside investigation service that provides information on the Proposed Representative that is available from public records.

a. Does the report indicate that the Proposed Representative has been involved in any civil litigation or administrative or criminal proceedings?

Yes ☐ No ☐

If Yes, provide details.

b. Do public records confirm representations made by the Proposed Representative concerning its business (location, size, owners, etc.) in the Proposed Representative Questionnaire?

Yes ☐ No ☐

If No, provide details.

8. If available, obtain and attach a Dunn & Bradstreet report (or an equivalent independent business assessment) on the Proposed Representative.

9. Will the Proposed Representative receive compensation for the services described in the attached agreement that is higher than the normal rate for such services?

Yes ☐ No ☐

If Yes, what justifies the extra compensation?

10. Will any part of the Proposed Representative's compensation be contingent upon the occurrence of any future event (for example, a consultant's fee linked to successfully obtaining a government permit)?

Yes ☐ No ☐

 

If Yes, provide the amount of the contingent compensation, describe the contingency, and explain the reason why compensation has been structured in this manner.

11. Will there be any other unusual provisions in the agreement with the Proposed Representative?

Yes ☐ No ☐

If Yes, describe those unusual provisions and explain their justification.

12. Have other Company business units had any dealings with the Proposed Representative?

Yes ☐ No ☐

If Yes, list those business units and describe the nature of the dealings.

13. Attach copy of the draft agreement with the Proposed Representative.

14. Are any of the following circumstances present:

- A regulator or other government official recommended Proposed Representative.
- Proposed Representative's suggested fee is much greater than the normal rate for comparable work.
- Proposed Representative's compensation includes a success fee that depends on some favorable action by a government agency or official.
- Proposed Representative has refused to agree to the anti-corruption provisions.
- There are indications that the Proposed Representative may have made improper payments to government officials in the past.
- Proposed Representative has requested unusual payment arrangements, such as being paid in cash or in a bank account that is located in a country other than the country in which the services would be performed.

Yes ☐ No ☐

 

If Yes, the Company may not enter into an agreement with Proposed Representative without first consulting with Global Compliance. You also must ***SEEK ADVICE*** if you are in any way unsure of the propriety of entering into an agreement with the Proposed Representative.

Signature: _____ Date: _____

Name: _____

Position: _____

## Section B: Approval

I have reviewed the foregoing information and collected supporting information as necessary, in order to assess whether this transaction complies with the Company's policies. Based on my review this transaction is

☐ APPROVED ☐ DENIED.

Signature: _____ Date: _____

Name: _____

Position: _____

Signature: _____ Date: _____

Name: _____

Position: _____

Compliance with Anti-bribery and Anti-corruption Laws

REPRESENTATIVE understands and will comply with all laws prohibiting bribery and corruption in performing this Agreement and any other agreement or understanding between the parties.

REPRESENTATIVE certifies that no officer, director, shareholder or owner of the REPRESENTATIVE's business is a government official or is related to a government official by blood, marriage or otherwise. If this situation changes, REPRESENTATIVE is obligated to notify the Company immediately.

REPRESENTATIVE, its officers, directors, stockholders, employees and agents, have not and will not pay, offer, or promise to pay, or authorize the payment, directly or indirectly, of money or anything of value to (a) any government, official, agent, employee of any government department or agency, or state-owned enterprise, whether or not acting in an official capacity; (b) any political party or official thereof or any candidate for political office; (c) any person knowing that all or any portion of such money or thing of value will be given or promised, directly or indirectly, to persons described in (a) or (b) for purposes of:

(1) influencing any act or decision of such entities or persons in their official capacity, including a decision to do or omit to do any act; or
(2) inducing such entities or persons to use their influence with any government or instrumentality thereof to affect or influence any act or decision of such government or instrumentality

in order to obtain or retain business with, or directing business to, the Company or to any person or entity.

REPRESENTATIVE agrees that all payments shall be made by check or wire transfer, and are payable in the country in which the REPRESENTATIVE resides or where the work is performed, and that all travel and entertainment expenses are to be reimbursed only when .
approved in advance and supported by detailed records.

REPRESENTATIVE agrees that s/he will not assign or subcontract work under the Agreement without the prior approval of the Company.

The Company may terminate the contract and/or withhold payment if it believes, in good faith, that REPRESENTATIVE has violated any law against bribery.

REPRESENTATIVE understands and agrees that its books and records related to performance of this Agreement are subject to audit by any Company official or representative, including, but not limited to outside auditors, accountants and lawyers. REPRESENTATIVE further understands that the terms of this Agreement may be disclosed to the United States government and its agencies as well as anyone else that the Company's General Counsel or Office of Global Compliance and Business Standards determines has a legitimate reason to know.

REPRESENTATIVE warrants and represents that it has received, reviewed, and agrees to abide by the Company's Bribery and Corruption policy, which is attached to this Agreement as Exhibit___.
REPRESENTATIVE will require all employees working on behalf of the Company to sign a certification (attached as Exhibit __) on an annual basis certifying compliance with the anti-bribery laws and Company policy.

 

Exhibit

**ANNUAL CERTIFICATION OF COMPLIANCE FOR INTERNATIONAL AGENTS, CONSULTANTS AND REPRESENTATIVES**

I _____ [name] a duly authorized representative of _____ _____ (the "Representative") do hereby certify for and on behalf of such company, that neither I, nor to my knowledge any other person, including but not limited to every other officer, director, stockholder, employee, representative and agent of Representative has made, offered to make, or agreed to make any loan, gift, donation or payment, or transfer of any other thing of value directly or indirectly, whether in cash or in kind, to or for the benefit of any official and/or political party, in connection with any business activity of the Company or any of its wholly or partially owned affiliates (collectively "the Company"). For purposes of this certification, the term "official" includes:

1. any employee or officer of any government, including any federal, regional or local department, agency, or enterprise owned or controlled by the government,

2. any official of a political party,

3. any official or employee of a public international organization,

4. any person acting in an official capacity for, or on behalf of, such entities: and

5. any candidate for political office.

I hereby confirm that should I learn any of the prohibited activities described above, or if there are any changes in the ownership or control of the Representative, I will immediately advise the Vice President of Global Compliance and Business Standards at ethics@consulate.com and the VP/Managing Director at _____.

I hereby confirm that neither I nor anyone else at the Representative company is a government official, nor am I related to a government official by blood, marriage or otherwise.

[REPRESENTATIVE]

_____

(Representative name)

Date: _____ By: _____

Name: _____

Title: _____

 

# ACC Annual Meeting

# Discussion of Consultate Corporation Hypothetical

Authors:

Ralph C. Martin, II
James P. Lucking
**Bingham McCutchen LLP**

Kevin J. Madden
Law Student

August 17, 2009

 

## Factual Background

Consultate Corporation is a publicly traded, multinational corporation headquartered in the US. The corporation provides public relations, advertising and reorganization consulting to a variety of clients, which are mostly manufacturers. Consultate has developed its government clients through a network of non-employee sales consultants.

Over the past three years, Consultate Corporation has become increasingly successful in advising companies in the developing world that are government owned but are now being privatized through the use of a proprietary consulting software program it has developed. The programs are adapted for specific clients but used throughout North America, Asia, and Europe. While the large number of privatizations has helped Consultate's business, Consultate has also suffered some drop-off in other business sectors and has laid off professional staff.

Richard Sarbox serves as General Counsel of Consultate Corporation. Sarbox reports directly to the CEO of Consultate, and has a dotted line report to the chair of the Audit Committee of Consultate's board of directors. One morning, he arrived at work and opened an email from Gloria Fedsupp, the office manager at the Albany, New York office. Fedsupp had received an anonymous email from a mass market service and forwarded the email to Sarbox. The email read:

> "Hey Glo, how's it goin? Headquarters still RIFing you? Ya know how badly Consultate is paying you? I do! I got hold of everyone's salary and bonus for 2008. Just check out the attachement. I might just email this to one of the business TV channels or blogs. Also, Im working for one of Consultates up and coming competitors – not telling ya who yet, and Im going after some of Consultates clients. Heck, with their software I can do the work for half what Consultate charges. Not worried about Consultate coming after me either. I know we only got that new Asian govt contract because our local guy and his rep paid off someone in the Ministry of Banking. Have a great life at Consultate!"
>
> Seeya!

Sarbox read the email and confirmed the accuracy of salary and bonus information and identified three main issues: (1) the writer, possibly an ex-employee, had stolen proprietary salary and bonus information; (2) the writer had stolen proprietary software and was planning to give it to a competitor; (3) an allegation that an agent of the company had paid a bribe to a foreign government official. Sarbox plans on initiating an internal investigation. This memorandum will address Sarbox's top priority questions.

## Initial Questions for Sarbox

**Does Sarbox have an immediate legal obligation to report the Foreign Corrupt Practices Act allegation to law enforcement?**

 

- The Foreign Corrupt Practices Act (FCPA) does not require disclosure of potential violations to U.S. enforcement authorities. However, legal obligations for potential violations of the FCPA do not stop with the statute itself.
    - The Sarbanes-Oxley Act of 2002,[1] created new certifications and SEC reporting requirements that may require Sarbox and Consultate to report the alleged violation.[2]
- After conducting an initial investigation to determine the scope and nature of the potential problem, Sarbox and Consultate should seriously consider voluntarily disclosing the allegation to law enforcement officials because it could lead to greater leniency and cooperation credit.
    - The Department of Justice, SEC, or other regulating bodies may discover the allegation and initiate an investigation. Disclosing the information to these law enforcement bodies before it becomes public may be worthwhile because it would indicate that Consultate is trying to address the problem.
    - The U.S. Sentencing Guidelines Manual provides guidelines on potential fines for violations of the Foreign Corrupt Practices Act anti-bribery provisions.[3]
    - The guidelines provide "cooperation credit" for voluntary disclosures.[4] "Cooperation credit" can reduce the amount of fines a company will have to pay if they have violated the FCPA.
    - In August, 2008, the Department of Justice published new guidelines for federal prosecutors who are engaged in the prosecution of a business organization for alleged criminal wrongdoing. The Filip Memorandum[5] ("Filip Memo") provides guidance for federal prosecutors on a number of issues, including voluntary

---

[1] Public Company Accounting Reform and Investor Protection Act of 2002, Publ. L. 107-204 (Sept. 30, 2002), codified at 15 U.S.C. §§ 7201-66 ("Sarbanes-Oxley").

[2] Sarbanes-Oxley requires CEOs and CFOs to certify that they are responsible for "effective internal controls," annual filings must report on the "effectiveness" of the internal controls and quarterly and annually reports must indicate any changes of corrective measures, CEOs and CFOs must disclose any "fraud" whether material or not to the auditors and board of direction, and requires CEOs and CFOs to certify that any SEC reports do not contain "untrue statement of material fact or omit to state a material fact." 15 U.S.C. §§ 302(a)(2)-(a)(6), 404(a).

[3] See the Foreign Corrupt Practices Act, 15 U.S.C. §§78dd-1(a), 78ff (prohibiting payments of anything of value to foreign officials for the purpose of gaining preferential treatment and penalizing such acts with a fine of $5,000,000 and the possibility of imprisonment for willful violations).

[4] See U.S. Sentencing Guidelines Manual §§ 8A, 8B (2008) (initiating a internal investigation and voluntary disclosure of potential violations are important factors).

[5] See Mark Filip, United States Department of Justice, Principles of Federal Prosecution of Business Organizations, available at www.usdoj.gov/opa/documents/corp-charging-guidelines.pdf. ("Filip Memo").

 

disclosure.[6] The memorandum states that the Department encourages companies to "conduct internal investigations and to disclose the relevant facts to the appropriate authorities."[7] While some executive and regulatory agencies have their own specific guidelines relating to cooperation credit,[8] they will often evaluate a company's compliance program and internal investigation in determining whether the company has taken the necessary steps to rectify any problems.[9]

- There are significant risks to a voluntary disclosure.
    - Voluntary disclosure of the allegation, setting aside any legal obligations to disclose, would raise serious issues of which Sarbox and Consultate should be aware:
        - Irrevocability: Once the disclosure is made to the appropriate law enforcement or regulating body, the company loses control of the situation and is at the mercy of the law enforcement body.
            - The allegation in the email may be an isolated incident, but if Consultate voluntarily discloses to a law enforcement body, there is a strong possibility that its investigation will expand and all of Consultate's business dealings could be investigated.
        - Collateral Risks: Voluntary disclosure may bring lawsuits from competitors, shareholders, and suspension or disbarment from government contracting opportunities.

[6] Id. § 9-28-750.

[7] Id.

[8] See "The Seabord Report," Exchange Act Release No. 44969 (Oct. 23, 2001).

[9] The Filip Memo also attempts to address concerns throughout the corporate and legal world that federal prosecutors would require companies to waive the attorney/client privilege and work product doctrine and refuse to indemnify officers and directors in exchange for cooperation credit. The Filip memorandum states that federal prosecutors should not evaluate cooperation credit on whether the business organization waived privilege protections, but rather upon the disclosure of "relevant facts concerning such misconduct." § 9-28-720. Many commentators do not believe that this change goes far enough because there will still be pressure to waive privilege claims if the privilege covers "relevant factual information."

 

**Does Sarbox have any immediate legal obligations to inform Consultate employees that their salary and bonus information has been compromised?**

- It is likely that courts will view salary and bonus information as private employee data because there is a reasonable expectation that the information would remain confidential.[10]

- The federal government has yet to pass a broad-based data privacy and security statute.

    - Several federal statutes provide privacy protections for personal information,[11] but they are limited in two distinct manners:

        - Regulations only cover certain information and certain types of entities.[12]

        - There is no federal standard for breach notification.

- Several states have enacted legislation requiring businesses maintaining computerized private employee data to notify the individuals of a security breach immediately.[13] States with similar statutes may require Sarbox and Consultate to disclose to employees the breach of private information.

---

[10] Although there is no single universal legal definition of private employee data, it generally includes an employee's name, in combination with his or her Social Security number, driver's license number, passport number, financial account number, credit or debit card number, health insurance identification number or other U.S.-government issued identification number. See, e.g., Conn. Gen. Stat. § 42-471.

[11] The Americans with Disabilities Act (ADA), the Family and Medical Leave Act (FMLA), and the Health Insurance Portability and Accountability Act (HIPAA) seek to protect the confidentiality of an individual medical information. Additionally, Sarbanes-Oxley and the Financial Services Modernization Act (Graham-Leach-Bliley Act), protect individuals from unauthorized exposure of financial information. With that said, these laws do not impose an express requirement to notify or mitigate the effect of a breach.

[12] See generally 45 CFR § 160.103 (describing covered entities, usually exempting employers).

[13] See, e.g., CAL. CIV. Code §1798.82 (West 2008) (requiring "any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."). Under the statute, private employee data is defined as (i) social security number; (ii) California driver license number; (iii) credit, debit, or bank account numbers, including security and access codes, and passwords' (iv) medical information; and (v) health insurance information. According to the statute, personal information does not include information made available through general public records from the federal, state, or local government." Id. California's statute has become the model, with many states, including Illinois, having enacted similar legislation. 815 ILLS. COMP. STAT. 530 (2008).

 

- Two states, Michigan and Connecticut, require employers that collect certain personal information from their employees to safeguard the data, computer files, and documents containing the information from misuse by third parties.[14]

**Investigative Strategy**

**What first steps should Sarbox take to investigate?**

- Sarbox, as General Counsel of Consultate, has determined that an internal investigation is necessary. The investigation will have several parts.
    - **Internal Information**:
        - Sarbox will need to determine several important issues quickly.
            - What happened?
            - Who was involved?
            - What are the potential risks?
        - Consultate should have an established document retention plan already in place. These plans allow for compliance with various legislative and regulatory requirements requiring companies to retain certain documents. In addition, Consultate should have a document destruction program that will ensure documents and data that does not need to be retained is destroyed properly.[15] In wake of the allegations in the email, Sarbox should initiate a litigation hold.
        - A company is required to initiate a litigation hold when there is notice of litigation, government investigation, or a subpoena or similar information request.[16] Courts may also require a litigation hold if an investigation or

[14] See Mich. Comp. Laws § 445.84 (requiring employers to adopt policies to protect confidentiality of employee Social Security numbers); Conn. Gen. Stat. § 42-471 (requiring employers to adopt policies to protect confidentiality of employee Social Security numbers and more broadly requiring that employers safeguard "personal information.").

[15] See Obrien v. Ed Donnelly Enterprises, Inc., 2006 U.S. Dist. LEXIS 66633 (S.D. Ohio 2006) (rejecting any claims based on overwriting of electronic data in accordance with established procedures).

[16] Chan v. Triple 8 Palace, Inc., No. 03CIV6048, 2005 WL 1925579, at *4 (S.D.N.Y. Aug. 11, 2005) ("The obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation -- most commonly when suit has already been filed."); Wiginton v. CB Richard Ellis, No. 02-6832, 2003 U.S. Dist. LEXIS 19128, at *23-24 (D.Ill. Oct. 27, 2003) ("[o]nce a party is on notice that files or documents in their possession are relevant to pending litigation, the failure to prevent the destruction of relevant documents crosses the between negligence and bad faith, even where the documents are destroyed according to a routine document retention policy").

 

lawsuit is reasonably anticipated.[17] A party's failure to timely impose a litigation hold may result in sanctions and adverse inference charges relating to information destroyed due to the absence of a timely litigation hold.[18]

- Who should receive notice of the litigation hold should be determined on a case by case basis.
    - Notification to relevant employees may prompt an employee to initiate litigation against the company. Sarbox should only notify as many employees as necessary to conduct a thorough an effective investigation.
- What documents a company will retain will be determined on a case by case basis.
- A litigation hold notice should include:
    - The identify of the person or persons who are subject to the hold;
    - The fact the claim has been made or is anticipated;
    - Mandating compliance with the litigation hold;
    - Identification of categories of documents to be retained;
    - Identification of any timeframe; and
    - Specific instructions (electronic data, refrain from discussing the nature of the hold with anyone, who should be contacted if there are any questions).

---

[17] See Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162, 175 (S.D.N.Y. 2004) ("The obligation to preserve evidence arises when the party has notice that the evidence is relevant to the litigation or when a party should have known that the evidence may be relevant to future litigation."); Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212, 217018 (S.D.N.Y. 2003) (holding a duty to preserve evidence would arise prior to an EEOC charge if there were a uniform belief by key players that litigation is likely); Danis v. USN Communs., Inc., No. 98-7482, 2000 U.S. Dist. LEXIS 16900, at 108-09 (N.D. Ill. Oct. 20, 2000) ("party knows or reasonably should know [evidence] may be relevant to the pending or impending litigation"). The court will have the benefit of hindsight when determining if a company should have reasonably anticipated a litigation or investigation. See Broccoli v. Echostar Communications Corp., 229 F.R.D. 506, 511 (D. Md. 2005) (holding that since all evidence was destroyed, litigation should have been anticipated at the time of an initial informal complaint of mistreatment to the plaintiffs immediate supervisors regardless of the supervisors belief of a future investigation).

[18] See, e.g., Zubulake v. UBS Warburg, LLC, 229 F.R.D. 422 (S.D.N.Y. 2004) (court imposed adverse jury instruction, which directed jurors to presume that certain emails that were not produced would have contained information detrimental to the defendant); U.S. v. Philip Morris, 327 F. Supp. 2d 21 (D.D.C. 2004) ($2.75 million in sanctions imposed for discovery violations, including deletion of relevant emails).

 

- The Federal Rules of Civil Procedure do not address the obligation to preserve electronic information nor the standards for issuing a preservation order. However, several of the Advisory Committee Notes of 2006 to the amended e-discovery rules provide guidance.

    - Fed. R. Civ. P. 26, Advisory Committee Notes of 2006 states, "[a] party's identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence. Whether a responding party is required to preserve unsearched sources of potentially responsive information that it believes are not reasonably accessible depends on the circumstances of each case."

- Courts in Delaware and around the country have held that directors and officers have a duty to ensure that a company has a reporting system "adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations," and that liability may hold where there is a "sustained or systematic failure of the board to exercise oversight [.]"[19] By informing officers and directors, Sarbox will allow them to address their compliance programs and oversight procedures early on.

- An effective internal investigation will encourage leniency and cooperation credit in any potential prosecution. Indeed, "[i]n determining whether to charge a corporation and how to resolve corporate criminal cases, the corporation's timely and voluntary disclosure of wrongdoing and its cooperation with the government's investigation may be relevant factors."[20] Moreover, "[e]ligibility for cooperation credit is not predicated upon the waiver of attorney-client privilege or work product protection."[21]

- Sarbox should decide whether to retain outside counsel. Based on the allegation and potential of criminal penalties and the extensive

---

[19] See In re Caremark International, Inc. Derivative Litig., 698 A.2d 959, 970-71 (Del. Ch. 1996) (finding no breach of a fiduciary duty because the officers and directors were aware of and took an active role in the company's compliance program and internal investigations); McCall v. Scott, 239 F.3d 808, 819 (6th Cir. 2001) (holding that directors could be held liable where "the failure of these directors to act was the result of an intentional or reckless disregard of 'red flags' that warned of the systematic fraudulent practices"); In re SFBC Intern. Inc., Sec. and Deriv. Litig., 495 F. Supp. 2d 477, 484-85 (D.N.J. 2007) ("lack of good faith can be established by a sustained or systematic failure of the board to exercise oversight."); Benjamin v. Kim, No. 95-9597, 1999 WL 249706, at *13 (S.D.N.Y. Apr. 28, 1999) (denying defendant's motion for summary judgment because plaintiffs had presented evidence that defendant's "actions constituted a total failure to exercise reasonable oversight").

[20] See Filip Memo § 9-28-700.

[21] Id. at 9-28-720.

investigation (foreign countries), Consultate Corporation would be advised to retain outside counsel.

- Outside counsel needs only to be retained when the scope of the investigation is too large or complex for in-house counsel and the company wants to ensure independence.

- Courts are more likely to apply the attorney-client privilege and work-product doctrine to communications and documents produced and exchanged between outside counsel and individuals of the company.[22]

- Experienced counsel tend to have greater experience with performing internal investigations and will be alert to the risk of potential conflicts. Additionally, outside counsel tend to have greater experience in dealing with government prosecutors and regulators, and will be less likely to succumb to pressure to waive privilege.[23]

- By retaining outside counsel to perform the internal investigation, Consultate will likely be able to demonstrate to prosecutors that they implemented an effective and independent compliance program and will be more likely to obtain leniency under the United State Sentencing Guidelines.[24]

- Personal Data

  - As discussed above, specific states and some federal laws have specific requirements relating to the protection of personal data. In addition, some states require companies to notify individuals, including employees, if there personal information has been breached.

---

[22] See Upjohn Co. v. United States, 449 U.S. 383, 390-95 (1981) (attorney-client privilege covers information from all corporate employees). In-House Counsel communication are frequently considered business advice rather than legal advice and thus are not protected by the attorney-client privilege or work product doctrine. See, e.g., In re Sealed Cases, 737 F.2d 94, 99 (D.C. Cir. 1994) (stating that an in-house counsel was a company vice president and had responsibilities outside legal sphere, company could shelter his advice only upon clear showing that it was given in professional legal capacity); Neuder v. Battelle pacific Northwestern Nat'l Lab, 194 F.R.D. 289, 295 (D.D.C. 2000) ("[i]n cases that involve in-house counsel, it is necessary to apply the privilege narrowly and cautiously lest the mere participation of an attorney be used to seal off disclosure").

[23] Although the Filip Memo stresses that waiver of attorney-client privilege and work product doctrine is not required to retain cooperation credit, commentators believe that prosecutors will still try to pressure companies to waive both privileges.

[24] See U.S. Sentencing Guidelines Manual §§ 8B2.1, 8C2.5 (2008) (stating that an internal investigation is a part of an effective compliance program).

 

- Employees may have standing to bring a claim against Consultate for exposure of their lost personal data.[25]

- Consultate should be aware of the potential for liability for misrepresentation in connection with the electronic data security breach.[26]

- Consultate could also face potential Federal Trade Commission action for failing to take reasonable and appropriate security measures to protect sensitive financial and medical data.[27]

- Injunctive Relief-Protection of Trade Secrets

  - The email raises concerns about the vulnerability of Consultate's proprietary software. The software will likely fall under the protection of a company trade secret, as defined by the Uniform Trade Secrets Act.[28] The software program is essential to Consultate's business.

  - The software program is likely a legally protected trade secret. In some jurisdictions, including both Illinois and New York, courts have held that, under the "inevitable disclosure" doctrine, an injunction may issue where a former employee's new employment "will inevitably lead him to rely on [his former employer's] trade secrets."[29]

---

[25] See Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (finding plaintiff had standing in a "lost-data" to assert a negligence and contract claims); but see Randolph v. ING Life Ins. And Annuity Co., 486 F. Supp. 2d 1, 6-8 (D.D.C. 2007), Key v. DSW, Inc., 454 F. Supp. 2d 684, 690 (S.D. Ohio 2006) (holding plaintiffs lack standing because they did not suffer an injury-in-fact sufficient to confer Article III standing).

[26] See In Re TJX Cos. Retail Sec. Breach Litig., 20007 U.S. Dist. Lexis 92782 (D. Mass. Dec. 18, 2007) (refusing to dismiss negligent misrepresentation claims based on misrepresented facts by TJX relating to its compliance with and implementation of security standards).

[27] In the Matter of CVS Caremark Corporation, 072 F.T.C. 3119 (2009) (consent order requiring CVS to improve security protections and pay a fine of $2.25 million).

[28] The Uniform Trade Secrets Act is a model law that has been adopted by 46 states. It defines "trade secrets" as: "Information, including a formula, pattern, compilation, program, device. . . that (i) derives independent economic value, actual or potential, from not being generally known to , and not being readily ascertainable by proper means, by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." Uniform Trade Secrets Act §1 (2) (1985).

[29] PepsiCo, Inc. v. Redmond, 54 F.3d 1262, 1269 (7th Cir. 1995); see also Strata Marketing, Inc. v. Murphy, 740 N.E.2d 1166, 1178 (Ill. App. Ct. 2000) ("We believe PepsiCo correctly interprets Illinois law and agree that inevitable disclosure is a theory upon which a plaintiff in Illinois can proceed[.]"); International Business Machines Corp. v. Papermaster, 2008 WL 4974508, at *10 (S.D.N.Y. Nov. 21, 2008) ("the likely inevitability of even inadvertent disclosure is sufficient to establish a real risk of irreparable harm to IBM"); DoubleClick, Inc. v. Henderson, 1997 WL 731413 (Sup. Ct. N.Y. Nov. 7, 1997) (enjoining a former employee from competing for six months, despite no restrictive covenants, due to the high probability of the future misuse of a trade secrets).

 

- Foreign Corrupt Practices Act
  - The email clearly alleges some potential violation of the Foreign Corrupt Practices Act.[30] The purpose of the act is to criminalize illicit payments to foreign public officials by U.S. businesses and individuals.
  - There are two parts of the act. The anti-bribery provisions[31] and the accounting provisions.[32] Each carry their own requirements and penalties.
  - Violations of the Foreign Corrupt Practices Act anti-bribery provisions are primarily investigated and prosecuted by the Department of Justice. Violations of the accounting provisions are investigated and prosecuted by the Securities and Exchange Commission.
  - Sarbox and Consultate will need to perform an initial investigation to determine the veracity of the email's allegation and the implications it will have on both parts of the Foreign Corrupt Practices Act. Failing to address potential issues early on will likely lead to increased penalties and fines.

**Who should Sarbox interview first?**

- Before any interview is conducted, Sarbox, in-house and outside counsel (if retained) should fully prepare for the interview by conducting background research and thoroughly reviewing all relevant, internal documents. The interview is one of the most important parts of an internal investigation because:
  - Counsel obtains relevant facts;
  - It is the foundation for the application of the attorney-client privilege and the work product doctrine. The information learned and disclosed during this investigation may be protected from discovery and disclosure to adverse parties and the government; and
  - It allows counsel to assess the credibility of employees in preparation for potential litigation.

---

[30] 15 U.S.C. §§ 78 et seq.

[31] See id. (These provisions make it a felony for any individuals to make a corrupt payment to a foreign official and apply to publically traded companies). Consultate uses non-employees in foreign countries to develop relationships with government officials. The actions of these employees may implicate Consultate under the anti-bribery provisions.

[32] See 15 U.S.C. § 78m (amended sections of the 1934 Securities Exchange Act and added additional record keeping and disclosure requirements for certain entities). These provisions require companies to keep accurate and up-to-date books and institute internal accounting controls to assure transactions are authorized.

 

- The schedule of interviews will be case specific. Consultate has more flexibility concerning the order of the interviews because it has initiated the investigation. Other factors, such as time restrictions and government subpoenas, will dictate the order of interviews. After conducting a thorough preparation, Sarbox or retained counsel should consider several issues that will influence the pace, structure, content, and order of the witness interviews. These issues are:
    - The purpose of the investigation.
        - Sarbox and Consultate Corporation are conducting this investigation to determine if there is any merit to the bribery allegation and how proprietary information (salary/bonus and software) was compromised.
    - The potential legal issues.
        - The interviews need to shed light on any peripheral legal issues and potential defenses the company will need to address and employ to protect from civil and criminal liability.
    - The potential uses of the investigation's findings and work-product.
        - Sarbox and retained counsel (if necessary) will need to use the information learned from the interviews to strategically and effectively discover the cause of the misconduct. After they have discovered the cause in the misconduct, they will be able to address any flaws in Consultate's current compliance programs.
    - Risks of addition adverse litigation.
        - There is a risk that Consultate's competitors will become aware of the investigation and inquiries and initiate adverse litigation. During the course of the interviews, employees and others privy to the internal investigation might discuss it with individuals outside the company. This information might find its way to a competitor of Consultate. Sarbox and counsel will need to strategically select which individuals to interview, and the timing and potential disclosure/leaking of the interviews should be considered to reduce the risk of unnecessary exposure. Additionally, the investigative attorney should remind individuals to not discuss the scope, purpose or existence of the investigation.
        - Investigating attorneys should warn employees before conducting the interview that they do not represent the individual.[33]

[33] MODEL RULES OF PROF'L CONDUCT, R. 1.13(d) (2008). Additionally, Model Rule 4.3 requires a lawyer who is dealing with an unrepresented person to "make reasonable efforts" to inform the individual that the lawyer represents another person and not the individual. Id. R. 4.3.

 

- The instructions should include:
  - The investigation attorney is conducting the interview to determine the legal rights and obligations of the company.
  - This is confidential and the employee is expected to keep the interview confidential.
  - Information learned in the interview will be shared with the company.
  - The interview is covered by the attorney-client privilege, but that privilege belongs to the company and may be waived at the company's discretion.
  - The investigating attorney represents the company, not the individual.
  - The company has the right to disclose the information to anyone, including the government.[34]
- These warnings are necessary, but Sarbox will need to prepare for the fact that an employee may be less inclined to disclose any information after this warning, especially if any disciplinary issues are probable.

- Employee contractual rights may limit their participation in an investigation. These issues often occur when an employee belongs to a union and there is a collective bargaining agreement which requires union representation during an investigation.[35]
- Absent a clear nexus between the government and a highly regulated entity, the federal constitution does not limit the powers of private employers in internal investigations.
  - Many companies are conducting internal investigations in accordance with federal statutes, such as FCPA and Sarbanes-Oxley, and a court could interpret an internal investigation

[34] Failure to provide these warnings in an unequivocal manner can put the company's privilege in jeopardy. In re Grand Jury Subpoena, 415 F.3d 333, 340 (4th Cir. 2005). These warnings have been labeled "Adnarim" warnings (Miranda spelled backwards).

[35] See N.L.R.B. v. J. Wingarten, Inc., 420 U.S. 251 (1975) (stating union employees have a right to demand a union representative if the investigation may result in discipline).

 

conducted to meet these statutory requirements to be a state action.[36]

- An employee has the right to speak to a lawyer before the investigation interview.
  - Under the Model Rules, an attorney can represent both the company and an individual if there are no conflicts and the appropriate consent of the company is secured.[37]
  - If an employee retains individual counsel, there are no legal obligations on the internal investigation team to consult with the employee's attorney prior to the interview. Sarbox and Consultate Corporation are advised that if an employee secures an individual attorney, they are better off to communicate with the employee's attorney in accordance with ethical requirements as a matter of precaution.[38]

- Allowing a Human Resources officer to sit in on employee interviews during the internal investigation will not be problematic.
  - Communications between employees of a company and counsel for the company at the direction of superiors seeking legal advice are covered by the attorney-client privilege.[39] The presence of a Human Resource officer will not jeopardize confidentiality because they are an employee of the client and are not adverse.[40]

**What internal records should Sarbox obtain?**

- Sarbox should obtain all documents relevant to the investigation. The type of documents a company retains during an internal investigation will be determined by the type and method of the investigation. Sarbox should try to obtain:
  - Documents that may be relevant to the bribery allegation:

---

[36] See Skinner v. Railway Labor Executives Ass'n, 489 U.S. 602 (1989) (finding a private railroad acted as a state agent in conducting drug tests in accordance with a federal statute).

[37] MODEL RULES OF PROF'L CONDUCT, R. 1.13(e).

[38] MODEL RULES OF PROF'L CONDUCT, R. 4.3 (2008).

[39] See Upjohn Co. v. United States, 449 U.S. 383, 390-95 (1981) (attorney-client privilege covers information from all corporate employees).

[40] United States v. Soudan, 812 F.2d 920 (D.Cal. 1986) (denying the attorney/client privilege because the third party was clearly adverse to the clients).

 

- Travel/expense reports;
- Electronic logs of phone calls made from internal phones and company-provided cell phones;
- Communications, both hard and electronic versions, between government officials and consultants in Asia;
- Documentation describing and authorizing service to be provided;
- Internal communication about all business relationships in Asia;
- List of recent dismissals/firings.

- Documents that may be relevant to the software theft:
  - Access logs;
  - Internal communications relating to the software;
  - List of recent dismissals/firings.
- Documents relating to the theft of salary and bonus information:
  - Access logs;
  - Human Resources/payroll documentation of salary information;
  - List of recent dismissals/firings.

- The purpose of obtaining internal records is to gather information relating to the bribery allegation, thefts, and also legal rights protecting company trade secrets. The document review needs to provide investigators with a comprehensive review of the company and as such, Sarbox should consider enacting some of the following policies:
  - Inform employees of the internal investigation and provide them with clear, understandable, written instructions of the type of documents that should be retained.
  - Establish an efficient and effective document gathering policy to ensure the comprehensiveness of the review and to protect against duplication and other mistakes.

 

- Employees, especially the IT Department, should be contacted and told to suspend any destruction or deletion process connected with Consultate's document retention policy.[41]

- Privileged documents should be segregated to maintain privilege status and to protect from inadvertent disclosure.[42]

    - During the document gathering and retention process, Sarbox should ensure that proper precautions are established to protect attorney-client and work product privileges.[43]

**Pro-Active Investigative Steps**

**Can Consultate secretly monitor employee telephone conversations and email?**

- It is a federal crime to intentionally wiretap or electronically eavesdrop on the conversation of another without a court order or the consent of one of the parties to the conversation.[44] It may also be a state crime to engage in such eavesdropping without the consent of one of the parties to the conversation.[45] Moreover, in eleven states, it is a state crime for anyone other than the police to engage in such eavesdropping without the consent of all of the parties to the conversation.[46]

- Generally, Consultate has the right to monitor an employee's emails when the employee is using company owned technology and has consented to a monitoring policy.[47]

---

[41] See 15 U.S.C. §7245; 18 U.S.C. §1519 (Sarbanes-Oxley documents retention requirements and penalties for failing to retain certain documents); In re Prudential Ins. Co. Sales Practices Litig., 169 F.R.D. 598, 617 (D.N.J. 1997) (fining a company for improperly destroying electronic data that impaired plaintiffs ability to establish claims). See, e.g., 29 C.F.R. §§ 1602.14, 1627.3 (requiring retention of certain personnel documents for a requisite length of time).

[42] See Hardy v. New York News, Inc., 114 F.R.D. 633, 645 (S.D.N.Y. 1987) (denying privilege to documents that were not marked as privilege and intermingled with other non-privileged documents). Counsel and investigators should clearly make and label documents as privilege and stored in a secure location.

[43] See In re Sealed Case, 877 F.2d 976, 980 (D.C. Cir. 1989) (inadvertent disclosure of documents will waive attorney-client privilege).

[44] 18 U.S.C. § 2511(1)(a),(b).

[45] See, e.g., New York Penal Law § 250.

[46] See, e.g., Mass. Gen. Laws ch. 272, § 99.

[47] See United States v. Grenier, 235 Fed. Appx. 541 (9th Cir. 2007) (employee consented to the company internet policy that allowed the company to monitor internet access).

 

- Under the Electronic Communications Privacy Act of 1986,[48] an employer is not allowed to intercept electronic communications from employees. If the employee is using company owned technology (email system, computer terminal) or is conducting communications with a client relating to the business, however, the company can monitor these communications for quality control and other business related reasons.
    - There is limited case law on the issue, but employees will likely be allowed to monitor employees' communications, especially email, if they are sent through a private employer's system.[49]
    - If Consultate does not have an established e-mail or technology policy, it should institute one immediately. The policy should contain specific language whereby the employees consent to the monitoring and a statement of business reasons for this activity.[50]
- Personal emails and telephone conversations raise additional questions. Two recent cases have expanded employee privacy rights in private communications.[51] Based on these cases, Consultate will not be able to monitor personal emails and telephone conversations.

**Can Consultate search employees' offices?**

- The type of search conducted by the Consultate will determine if it will withstand Fourth Amendment scrutiny. A private employee "retains at least some expectation of privacy in their offices."[52]
    - An expectation of privacy from search will generally arise when an employee is allowed to lock a desk, drawer, locker and keep the key.

---

[48] 18 U.S.C. §§2510-2720.

[49] See id. (monitoring done in the normal course of business or to protect the employer's rights or property).

[50] A court has found that a company did not violate the privacy rights of its employees when it intercepted e-mail communication. The court found that if there is a public safety purpose for the interception, no privacy rights are violated. Smyth v. Pilsbury Comp., 914 F. Supp. 97 (E.D. Pa 1996).

[51] In Hay v. Burns Cascade Co. Inc., 2009 U.S. Dist. LEXIS 12160 (February 18, 2009), the court held that a company had invaded the privacy of an employee by monitoring a personal telephone call with the employee's husband. The court stated that the employer had failed to properly inform the employee that the calls were being monitored. Similarly, in Van Alstyne v. Electronic Scriptorium, Ltd., 560 F.3d 1999 (4th Cir. 2009), the court held that a company president could not monitor the personal email of an employee in violation of the Stored Communication Act.

[52] United States v. Zeigler, 474 F.3d 1184 (9th Cir. 2007).

 

- If any employee refuses to allow the search, Consultate may be within its right to discipline or terminate an employee for failing to cooperate.[53]

**Can Consultate conduct background investigations of employees? Former employees?**

- An employer can conduct background checks on current and prospective employees.[54]
  - Under the Fair Credit Reporting Act,[55] if the employer uses an outside company (including a law firm) to conduct the background investigation, they must provide advance written notice, and prior to any adverse action, it must disclose the report to the employee.[56] If the background investigation is conducted in house, then no notice or disclosure is required.
  - If an investigation is conducted by a third party group due to an allegation of employee misconduct, no notice is required and adverse action against the employee can be taken before the report is disclosed.[57]

**Can Sarbox compel an employee to answer questions on penalty of dismissal?**

- There is an implied duty of loyalty and cooperation in the employee/employer relationship.
- Sarbox should consult the company's HR polices and handbook as well as the employee's contract (if any) to determine if there are any collective bargaining restrictions that would prohibit threatening dismissal.
- Under many state laws, Sarbox and Consultate can terminate an employee for failing to cooperate in an internal investigation if they can show "good cause."[58]

---

[53] See TRW, Inc. v. Superior Court, 31 Cal. Reptr. 2d 460 (Cal. Ct. App. 1996); Easterson v. Long Island Jewism Med. Ctr., 156 A.D.2d 636 (N.Y. Gen. Term 1989) (dismissing employees for failing to cooperate did not violate public policy or state law).

[54] Several states will hold employers liable for the actions of their employee. Claims can be brought against the employer if they are negligent in their hiring practices and do not complete the proper review of the potential or current employee.

[55] 15 U.S.C. §§1681 *et seq.*

[56] 15 U.S.C. §§ 1681b(2)(A), 1681b(3)(A).

[57] This section was added when the Fair Credit Reporting Act was amended in 2003. The Fair and Accurate Credit Transaction Act, Pub. L 108-159, 111. Stat. 1952.

[58] See Pugh v. See's Candies, Inc., 116 Cal. App. 3d 311, 330 (1981) (defining good cause as "a fair and honest cause or reason, regulated by good faith on the party of the party exercising the power").

 

- Generally, Sarbox cannot terminate the employee for any arbitrary, capricious, or illegal reasons.[59]

- In this case, the employee was willing to answer questions about his working relationship with former employees and terminating him because he refuses to discuss private information may be considered arbitrary and capricious. Without describing a legitimate business reason for the termination, Sarbox and Consultate will not have good cause.

**Can Consultate legally and ethically promise its former employee that it will not "prosecute" him for sending the emails?**

- Consultate cannot promise not to prosecute the former employee because it cannot speak on behalf of a government entity, such as the local district attorney's office. The decision to prosecute rests solely with the appropriate government authority.[60]

- Whether Consultate reports the former employee to the authorities will depend on whether it has a legal duty to do so under the statutes discussed above. In the wake of Sarbanes-Oxley, there is greater pressure on companies to report and disclose any information that may have a negative affect on the stock price.

    - Even assuming no legal duty to report exists, Consultate will have to balance a number of competing interests in deciding whether to report the former employee. A vote by the board of directors could decide that it is not in the company's business interests to report the former employee or to publicize the issue because it will negatively affect the company's stock price. Under the business judgment rule, a company has to be grossly negligent in its decisions for liability to attach.[61] Deciding not to report the former employee will not likely violate the business judgment rule and Consultate could legally and ethically make the deal.

[59] Contran v. Rollins Hudig Hall Int'l Inc., 17 Ca. 4th 93, 108 (1998).

[60] See People v. Kurz, 847 P.2d 194, 196 (Colo. Ct. App. 1992) ("The decision to prosecute is within the exclusive province of the district attorney.").

[61] See generally DEL. CORP. LAW §102(b)(7).

 

# Conducting Corporate Investigations

## *The Use of Lawful and Ethical Strategies*

*Presented at:*

**Association of Corporate Counsel Annual Meeting**
**Boston, MA**
**Tuesday, October 20, 2009**
**9:00AM – 10:30AM**

*Prepared by:*

John Lewis, Jr.
Senior Managing Litigation Counsel
The Coca-Cola Company

and

Joy T. Davis
Class of 2010
Walter F. George School of Law
Mercer University

 

# Conducting Corporate Investigations

For in-house lawyers, particularly in-house litigation counsel, proper structuring and leading of internal investigations is critically important. A well run internal investigation can root out compliance gaps, bolster investor/management confidence and dissuade government authorities from taking separate action. On the other hand, a poorly run internal investigation can worsen things by generating negative publicity and encouraging civil litigation by people who learn of corporate wrongdoing.

This paper examines the ethical considerations in conducting an internal investigation including whether or not to retain an outside firm, and the proper documentation of corporate records during the investigation. Employee interviews, the importance of *Upjohn* warnings and how to properly handle requests by employees to speak to a lawyer are also discussed. Proper structuring of priority issues at the outset ensures ethical and effective investigations.

## I. Handling the investigation internally or retaining an outside firm.

There are several factors to consider in making the decision to hire outside counsel to conduct an internal investigation. Retention of an outside firm gives the investigation the perception of independence and access to specialized counsel who may have more expertise in dealing with the relevant federal and state laws. The perception of independence may be further magnified if a firm with little or no prior association with the company is used versus a regularly used law firm. Further, the use of an outside firm prevents potential strain on important working relationships between those conducting the investigation and colleagues in the company. Using an outside firm would also assure that in-house counsel is not pulled from ongoing tasks, and prevents implication of a “whitewash” if in-house counsel was relied upon, consulted or involved in the matter being investigated.

 

If the decision is made to utilize in-house counsel to conduct the investigation, two areas of major concern are Attorney-Client Privilege and Work Product Doctrine. Attorney-Client Privilege applies to the work of in-house counsel,[i] but in the United States, if the in-house counsel conducting the investigation is also performing an "advisory business function", and has other non-legal functions that are relevant to the investigation; it is possible that investigation communications will not be protected. For example, a District of Columbia circuit court[ii] held that communications to and from in-house counsel were not protected by attorney-client privilege where the in-house counsel had responsibilities outside the legal sphere. Ensuring that in-house counsel performs no other function, other than legal functions, will protect against inadvertent waiver of attorney-client privilege.

When the investigation is conducted using in-house counsel, special attention to how the progress of the investigation is documented will assure protection under the Work Product Doctrine. The Work Product Doctrine applies to in-house counsel,[iii] but not all materials prepared or obtained with an eye toward litigation will necessarily be protected and may properly be discoverable under *Upjohn.*[iv] Memoranda should be properly marked if confidential, and should reflect the mental impressions of the lawyer. One of the main advantages of using in-house counsel is that they will likely have a fuller understanding of the corporation's business. While an intimate understanding of the business has the potential of making an investigation more efficient and effective, the same understanding of the business makes the in-house lawyer an attractive fact witness and ultimately places the privileged nature of the investigation at greater risk.

The Model Rules of Professional Conduct provide guidance for many ethical considerations during an internal investigation. Under Rule 1.2(a) a lawyer should structure the

 

scope of an investigation at the outset to determine what the investigation seeks to accomplish. Having a clear scope will assist with setting goals, and determining when goals have been met. In conducting the investigation, Rule 1.3 requires that a lawyer acts with reasonable diligence and promptness. Keep in mind that as in-house counsel you might be investigating friends and colleagues. Consideration must be given to whether you may become a witness in the investigation. Under Rule 3.7, a conflict is created if in-house counsel is a witness in the transaction or activity under investigation. Finally, under Rule 5.5 and Rule 8.5 consider that as a lawyer you may not be admitted in the jurisdiction where you conduct the investigation. This becomes more of an issue where portions of the investigation are conducted outside the United States. Determine which rules apply during the investigation, and make sure that you are aware of all the relevant rules that impose obligations on you as a lawyer.

## II. Obtaining corporate records.

When conducting an internal investigation, the manner in which corporate records are identified, secured and reviewed are vital to the success and legitimacy of the investigation. Keep in mind that all documents created, facts uncovered and witness statements may have to be disclosed to the government, and may ultimately be discoverable to the employee.[v] In setting up corporate record retention procedures consider suspending normal retention procedures. For example, your company may be discarding or overwriting computerized information in the ordinary course of business. In designing a "search" for relevant corporate records, ascertain the types of documents routinely generated by the corporation, including relevant foreign offices. An understanding of the types of records generated is important because relevant documents may exist, that are not identified by employees, and knowingly withholding or the destruction of documents may be viewed as obstruction of justice.[vi] Identify the company personnel likely to

 

possess relevant documents, for example employees with access to information regarding software development and storage; personnel records, salary and bonus information; communication with foreign governments etc., and their position on the company organizational chart. Remember to review copies of calendars, compliance manuals, training materials, and job descriptions for the period of time covering the investigation as they may provide valuable insight. Documents may be organized in a spectrum, from irrelevant to crucial, by key topic or chronologically. Proper organization and review of identified documents will maximize efficiency. Finally, a log should be created to identify location where each document was obtained.

If a parallel government investigation is likely to occur, carefully consider the pros and cons of putting findings into a written report, as these reports may become discoverable. One on one verbal briefing with senior executives who are not, themselves, fact witnesses or potential targets of the investigation is the better practice. Also decide early on whether, and how, you will "cooperate" with the government keeping in mind that self-policing, self-reporting, remediation, and cooperation are paramount factors in determining enforcement against a company by the government.[vii] Further, Department of Justice guidelines indicate that a corporation's timely and voluntary disclosure of wrongdoing, and waiver of legally protected attorney-client and work-product doctrine privileges will result in favorable treatment during an investigation.[viii]

 

## III. Interviewing employees.

Before you begin conducting interviews, determine the order in which you will interview employees, as well as the techniques and methods you will use. Concentric order is advisable - starting with those less involved and moving to "key" witnesses. However, if there is an identified wrong-doer, start with their interview first. The advantage to interviewing a wrong-doer first is that they will be "locked" into their story and will not easily be able to change it later. Decide ahead of time what format the interview will follow. Be flexible and avoid questionnaires unless the information sought is objective, to allow for fuller communication. Assemble interview teams that have at least two lawyers present for each interview in case it is necessary to corroborate the recollections of the one of the lawyers. Having two interviewers will also allow one of the lawyers to take notes. Notes should be of the lawyers "mental impressions" and not a substantially verbatim record of the interview. Consider setting up "separate issue" teams and put the best talent where it will benefit the interview the most. Finally, outline for those conducting the interview what techniques and methods are acceptable, as well as those that are not.

The presence of a Human Resources (HR) representative is sometimes an option during employee interviews. While the presence of an HR representative may be routine practice when a company lawyer interviews an employee, consider that the presence of other company employees may have a chilling effect on the employee's candor. Further, the presence of HR may result in the interview being construed as having a "business purpose" and losing protection under the work product doctrine. Additional considerations include the requirement under the Models of Professional Conduct Rule 5.3 that the HR employee complies with the investigation's standards and the Rules of Professional Conduct. Compliance with Rule

 

5.7(a)(2) is especially important, and the investigating lawyer must make sure that the employee understands that the HR representative also represents the corporation and cannot provide legal assistance to the employee. Finally, when establishing the format and techniques to be used during interviews, consider company policies, and the perceptions of the public, media, government and other stakeholders.

The Model Rules of Professional Conduct provide additional guidance for shaping your interview process. Once the interview process has been established, Rule 1.2(a) requires that the lawyers conducting the interviews abide by the methods, techniques and objectives of the process. Additionally, Rule 4.4 requires that reasonable techniques/methods be used in conducting interview. Rule 1.4 requires prompt, clear communication with the corporation regarding decisions and progress made. Information obtained through the interview of employees that sheds light on the transaction or activity being investigated must be kept confidential, unless the corporation authorizes disclosure as per Rule 1.6. Finally, Rule 3.4 requires the lawyer to act fairly towards the employee.

Before any employee is actually interviewed, they must be given *Upjohn*[ix] warnings. This is necessary in order to maintain attorney-client privilege between the corporation and the lawyer. *Upjohn* warnings serve two important purposes: first, the warnings aid the investigating lawyer in discharging his or her ethical duty not to mislead the employee. Second, the warnings reserve the attorney-client privilege solely for the corporation. In order for *Upjohn* warnings to be considered adequate, three specific warning should be given by the interviewing lawyer at the outset of the interview. First, the lawyer should unambiguously indicate that he or she represents the corporation, not the individual. Next, the interviewing lawyer should indicate that while the interview is covered by the attorney-client privilege, the privilege belongs to, and is controlled

 

solely by, the corporation.[x] Finally, the employee should be warned that the company may decide to waive the privilege in the future and may disclose certain information obtained from the employee in the interview to third parties and/or government investigators or prosecutors.

*Upjohn* warnings are especially important where the investigation is conducted by in-house counsel because it is more likely for an employee being interviewed by a lawyer whom they consider to be a "co-worker" to also represent their interests. As a final consideration once the employee receives appropriate *Upjohn* warnings and agrees to proceed with the interview, it may be necessary to obtain a written acknowledgement that the lawyer effectively communicated that they do not represent the employee prior to the interview.[xi]

The Model Rules require that an employee gives informed consent[xii] to be interviewed, and that they understand fully that the interviewing lawyer represents the interests of the corporation.[xiii] Rule 4.1 requires the lawyer to be truthful in all their statements to the employee, and if the employee is unrepresented, Rule 4.3 requires that the lawyer does not state or imply that they are disinterested. If the employee asks to speak to a lawyer first, the best course of action is to stop the interview immediately and allow the employee adequate time to obtain counsel. Rule 8.4 requires that the lawyer does not try to persuade the employee to continue with the interview, or minimize the fact that the lawyer does not represent the employee's interests.

## IV. Conclusion.

While there is no "one size fits all" approach to handling internal investigations, following recommended practices[xiv] will be helpful when navigating uncertain waters. There are numerous considerations at each step, and only meticulous planning will properly address

 

unanticipated traps. Lawyers conducting the investigations will have to adapt to the unique aspects of each investigation and remain flexible throughout the process.

---

[i] U.S. v. Rowe, 96 F.2d 1294, 1296 (9th Cir. 1996).

[ii] In re Sealed Case, 737 F.2d 94, 99 (D.C. Cir. 1984).
[iii] Rowe, 96 F.2d at 1296.

[iv] Upjohn v. United States, 449 U.S. 383, 399 (1981).

[v] *See* Id. (holding that under the Work Product Doctrine not all materials prepared or obtained with an eye toward litigation will necessarily be free from litigation, and may properly be discoverable).

[vi] *See, e.g.* United States v. Davis, 1 F.3d 606 (7th Cir. 1993) (client whose attorney represented to government that documents being produced were all the documents that responded to the subpoena was charged with obstruction of justice when the government learned of the existence of another document it determined was within scope of subpoena).

[vii] Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions, Exchange Act Release No. 44969 (Oct. 2001) *available at* http://www.sec.gov/litigation/investreport/34-44969.htm).

[viii] *See* U.S. D.O.J., Principles of Federal Prosecution of Business Organizations (Jan. 20, 2003) (the "Thompson" Memorandum"), *available at* http://www.usdoj.gov/dag/cftf/business_organizations.pdf. (The Thompson Memorandum was later revised by the "McNulty" Memorandum which requires that federal prosecutors seeking a corporate waiver of privilege first obtain written permission to see the waiver from the Deputy Attorney General)
[ix] *See* Upjohn v. United States, 449 U.S. 383, 386-396 (1981) (holding that client privilege is maintained between counsel and the client-corporation when the lawyer for the company communicates that the lawyer does not represent the employee, and represents the company as a legal entity).

[x] *See* In re Grand Jury Subpoena: Under Seal, 415 F.3d 333, 339-40 (4th Cir. 2005) (Holding that where the employee knows that the lawyer is representing the corporation alone, and that the employee is not the client, then the company alone holds the privilege).

[xi] *See* In re: United States v. Nicholas, No. SACR 08-00139-CJC (C.D. CA, April 1, 2009).

[xii] Model Rules of Prof'l Conduct R. 1.0 cmt. (2007) requires that employees must have information that is reasonably adequate in order to make an informed decision.

[xiii] *Id*. at Rule 1.13 (f). Employee must understand that the lawyer represents the organization if the employee's interests are adverse to those of the corporation.

[xiv] *Recommended Practices For Companies And Their Counsel In Conducting Internal Investigations*, (American College of Trial Lawyers, Feb. 2008) *available at* http://www.actl.com/Content/NavigationMenu/Publications/AllPublications/default.htm.

 

# ACC Extras

Supplemental resources available on www.acc.com

So, Your Corporation Has Been Sued? What to Do in the First 30 Days. InfoPak. March 2009
http://www.acc.com/legalresources/resource.cfm?show=208360

Please note, these additional resources are provided by the Association of Corporate Counsel and not by the faculty of this session.