

Corporate Counsel



Published by the Corporate Law Department Section of the Washington State Bar Association

Volume 14

Summer 2003

Number 1

Insider Trading **Who Is on the Move?**

Jennifer O'Connor has taken the position of VP and General Counsel at Puget Sound Energy. She was formerly Interim General Counsel for Starbucks. Ross Macfarlane has been hired as General Counsel at the Seattle Monorail Project. Mike Brandeberry also joined Washington Mutual as Senior Counsel and David Zilkie as Counsel. Mr. Zilkie moves to WaMu from GE Capital. Safeco has hired several new attorneys including Stephanie Daley-Watson, VP and Associate General Counsel; SoYoung Kwon, Corporate Counsel; and Sarah Dods, Corporate Counsel. Meena Kang Latta has moved from LoudEye to become the General Counsel of BSquare Corporation in Bellevue. Starbucks has made several recent additions to their staff. Wayne Michigami has become the Director, Corporate Counsel. Sean Dyers, formerly from Boeing is Corporate Counsel, and Catlin Moughon has moved from Riddle Williams to become their Director, Corporate Counsel. Carrie Schnelker has become the Manager Contracts for Nintendo of America, Inc.

Table of Contents

Insider Trading – Who Is on the Move?	1
Basic Noncompete Principles, Practical Tips and Best Practices	1
Quarterly Dinner Meeting Announcement	2
USA PATRIOT Act and Terrorist Financing Regulations: Beware Your Compliance Obligations and Strict Liability. 7	

Basic Noncompete Principles, Practical Tips and Best Practices

by Tahl Tyson – Davis Wright Tremaine LLP

Here are the some basic legal principles and best practices that employers can use to protect their business information from misappropriation and prevent unfair competition or, conversely, avoid being sued when hiring employees from competitors.

A. Restrictive Covenants.

1. Noncompetition Agreements.

Practical Pointers: Although some employers may feel apprehensive that they will risk losing potential recruits if they raise the issue of restrictive covenants, this fear is not well founded. Such agreements have become so commonplace that most employees expect them. Here are some practical pointers:

- Tell prospective employees up front that you will require a noncompete and confidentiality agreement.
- Be reasonable and clear in drafting the terms, which should be tailored to reflect what the employee will be doing for you. Take the time to customize noncompete agreements. Any ambiguity will be construed against the company.
- Be selective. Only employees with actual access to proprietary information should be required to sign them. A court may question the legitimacy of the employer's purported business interest if every employee at all levels has to sign off on the same boilerplate covenant. Employers should require those employees who do not genuinely require the added layer of protection that accompanies a noncompete

(continued page 3)

The Corporate Law Department Section

QUARTERLY DINNER MEETING

Tuesday, September 9, 2003



Location To Be Determined

*(most likely Spazzo Mediterranean Grill
in the Key Bank Building,
9th Floor, 10655 NE 4th, Bellevue, WA)*



**Social Period from 6:00 P.M. to 7:00 P.M.
(No-Host Bar)
Dinner at 7:00 P.M.**



Special Guest Speaker:

Robert Major

Mr. Major is a founder of the global attorney search consulting firm MAJOR HAGEN & AFRICA and will be providing his national and local perspective on the job market and employment-trend data of special interest to in-house counsel.

Information for Your Clients

Did you know that easy-to-understand pamphlets on a wide variety of legal topics are available from the WSBA? For a very low cost, you can provide your clients with helpful information. Pamphlets cover a wide range of topics:

- Alternatives to Court
- Bankruptcy
- Buying and Selling Real Estate
- Consulting a Lawyer
- Criminal Law
- Dissolution
- Elder Law
- Landlord/Tenant Rights
- Lawyers' Fund for Client Protection
- Legal Fees
- Marriage
- Parenting Act
- Probate
- Revocable Living Trust
- Signing Documents
- Trusts
- Wills

Each topic is sold separately. Pamphlets are \$9 for 25, \$15 for 50, \$20 for 75, and \$25 for 100. Pricing for larger quantities is available on request.

To place your order or for more information, please contact the WSBA Service Center at 800-945-WSBA or 206-443-WSBA. Sales tax is applicable to all in-state orders.

Basic Noncompete Principles, Practical Tips and Best Practices... continued from page 1

to sign off on a narrowly tailored confidentiality, and perhaps a no-customer solicitation and/or a no-employee poaching agreement.

- Make certain that the agreement is supported by adequate consideration, ideally when first hired, or when some other benefit is given to the employee.
- *Don't overreach.* Noncompetition agreements must be reasonable in scope, time and territorial restrictions, and no more restrictive than reasonably necessary for the protection of the company's legitimate business interests.

The General Rule: The general rule is that noncompetition agreements must, at a minimum, be reasonable in scope, time and territorial restrictions, and no more restrictive than reasonably necessary for the protection of the company's *legitimate business interests*. There must also be sufficient "consideration" (*i.e.*, something of value to which the employee would not otherwise be entitled) given for the employee's promise not to compete.

Legitimate Protectable Interest: An employer's legitimate business interest includes proprietary information or relationships (customers and, possibly, suppliers) which pertain to its operation and which an employee acquires during the course of employment. A noncompete will not be enforced where the employer is not protecting a legitimate business right, but is merely attempting to restrict the employee's ability to use skills learned on the job in future employment.

The employer's protectable interest determines both the enforceability and scope of the noncompete restriction. When determining whether a noncompete covenant is reasonable relative to the employer's interest, the scope of the restriction is considered from three perspectives: (1) whether the restraint imposed upon the employee is a greater restraint than necessary to protect the business or the goodwill of the employer; (2) whether the restraint imposed on the employee is a greater restraint than necessary to protect the employer's interest; and (3) whether the degree of injury to the public involves the loss of service and skill of the employee so as to warrant non-enforcement.

2. Confidentiality Provisions.

Confidentiality provisions can be used in addition to or in lieu of noncompetition provisions. Confidentiality provisions can define what information is protected

more broadly than does the trade-secret statute. Such provisions can also be helpful in enforcement litigation to demonstrate that the employee knew that misappropriated information was confidential. Confidentiality agreements are analyzed somewhat like noncompetes: they must be reasonable as to scope and time and be supported by sufficient consideration.

3. Nondisclosure Agreements ("NDA").

NDAs serve a similar function as confidentiality agreements, except that they are often used to protect trade secrets and proprietary information not only in the employment context, but in any situation where the information is being divulged to someone for a limited purpose. It could even be used, for example, in the context of a final stage interview of a prospective job candidate with whom a company needs to share some otherwise confidential information about its plans or products in order for the candidate and the company to determine whether they are a "match."

4. Nonsolicitation Clauses.

A restriction on soliciting and servicing customers can substitute for or complement a restriction on competitive employment, and is generally more enforceable than a noncompete. A court can limit the scope and duration of a nonsolicitation clause, or may enforce it only with regard to clients of an employer with whom the former employee actually came into contact in the course of his or her employment.

B. Trade Secrets.

Trade secrets are typically defined as one subset of intellectual property rights (others include patents, trademarks and copyrights). Such intellectual property has been traditionally described as intangible personal property which results from the fruit of mental labor. Courts continue to recognize that as a matter of fundamental fairness and common sense, one should be able to keep and enjoy the fruits of one's labor. A trade secret consists of any confidential information used in business, which gives the owner an advantage over competitors. Reasonable efforts must be made to keep the information secret. Obviously, information which is publicly known or available cannot be protected as a trade secret.

Forty-two states including Washington (RCW § 19.108.010(4)), have adopted the Uniform Trade Secrets

(continued next page)

Corporate Counsel is published quarterly for the benefit of section members. We welcome any comments you may have about its content or suggestions for future articles. Please contact Editor Dave Anderson at (206) 281-1005 (direct line), (206) 281-1444 (fax), or David.Anderson@Airborne.com (e-mail).

Basic Noncompete Principles, Practical Tips and Best Practices... continued from previous page

Act ("UTSA") in one form or another. Trade-secrets claims are particularly effective in litigation because the remedies available under the UTSA include injunctive relief for "threatened" misappropriation, attorneys fees, and double damages for "willful" misappropriation.

C. Common-Law Duties.

1. Employer Duty of Loyalty.

Employees are not permitted to undertake or participate in activities adverse to the interests of the employer *during the course of employment*. Examples of activities that are typically considered a breach of the duty of loyalty include soliciting the employer's customers for the employee's own benefit or the benefit of his or her new employer; luring away co-workers to a competing enterprise; failing to disclose matters adverse to the employer and that impair the employee's duty of loyalty; taking payments from a third party who is doing business with the employer; and divulging the employer's confidential information to others.

Although it is a breach of the employee's duty to set up and operate a competing business while employed by another, an employee may take limited, preparatory steps effective only upon termination of employment. Merely informing customers of one's former employer of a change of employment, without more, is not solicitation. Nor is making arrangements for office space, inquiring about benefits packages, investigating computer systems, and meeting with accountants in preparation for starting a competing business.

2. Duty of Confidence.

The employer-employee relationship gives rise to "confidences." The duty of an employee not to disclose the secrets of his or her employer may be implied from the confidential relationship existing between the employer and the employee. The nature of the relationship imposes a duty on employees and former employees not to use or disclose the employer's trade secrets. Based upon a breach of this confidential relationship, a court may enjoin an employee's use of an employer's confidential customer information even in the absence of an express restrictive covenant.

3. Inevitable Disclosure Doctrine.

The inevitable disclosure doctrine is a fairly new and controversial doctrine that has not been adopted by courts in Washington. The general concept, however, is often argued by employers seeking to prevent a key former employee from working for a direct competitor. The theory of the doctrine is that, in order to perform

his or her job for the new employer, the employee cannot help but disclose confidential information to the advantage of the new employer. It may be appropriate in a situation where the former employee competes directly with the new employer; the employee possesses highly confidential or technical knowledge concerning manufacturing processes, marketing strategies, and the like; the employee's new position is nearly identical to his or her old one; and the trade secrets or confidential information are valuable to both employers.

D. Business Torts.

Business torts, such as tortious interference with business relationships, interference with prospective economic expectancies, and interference with contract may also provide a non-contractual basis for claims involving particularly serious unfair competitive practices by former employees hired by competitors.

A former employer may have a claim of tortious interference against a new employer if the new employer places the employee in a position which results in the violation of the employee's noncompete agreement with the former employer. The Trade Secret Act, however, will preempt tort claims if the information sought to be protected rises to the level of a trade secret. If it does not, then business torts may come into play. In drafting a complaint, therefore, it is wise to include both types of claims, in the event that the court rules that the information at issue does not rise to the level of trade secrets.

E. Criminal Sanctions.

Problems arising from corporate espionage prompted Congress to pass the 1996 Economic Espionage Act (18 U.S.C. § 1831 *et seq.*). Under the Act, intentionally acquiring or knowingly receiving another's secrets through an ex-employee can result in criminal penalties. To avoid liability or reduce penalties under the Act, employers will need to show that they took appropriate steps and established genuine safeguards to reduce the risk that they would violate receive stolen secrets. Washington State also has criminal sanctions for misappropriation of trade secrets set forth at RCW 9A.56.010(5) and 9A.56.020.

F. Best Practices for Protecting Confidential Information.

1. Make Reasonable Efforts to Maintain Confidentiality in the Workplace.

In addition to confidentiality and noncompetition agreements, you should also consider having a formal, comprehensive plan to protect information and trade secrets. This will also help you in the event that you

(continued next page)

Basic Noncompete Principles, Practical Tips and Best Practices... continued from previous page

need to bring a lawsuit: because a trade secret plaintiff bears the burden to prove the alleged trade secret was subject to reasonable measures to maintain its secrecy, you must be able to show that you were consistently diligent in protecting the information.

- Determine what are truly trade secrets (essential data, processes, etc.) as opposed to other information.
- Educate employees to understand the difference between information that is proprietary or a trade secret, and other types of information.
- Explain the "work for hire" concept to employees, *i.e.*, that both the tangible and non-tangible intellectual work that they do belongs to the company.
- Adopt a written policy on trade secrets and confidential information and notify employees of this policy in an employee handbook or manual.
- Train employees to protect trade secrets. Such training can be incorporated into ethics training if your company already has this.
- Invest in physical security measures, such as locked filed cabinets, swipe-card systems, and the like and limit access to confidential information, areas where research and development is taking place, or customer lists.
- Design products to not reveal trade secrets upon inspection.
- Confidential documents should be clearly identified, with restrictions on copying and distributing. Take steps to ensure the security of computers and electronic media.
- Screen employee speeches and publications.

2. Talk to Departing Employees.

- **Conduct exit interviews.** Remind departing employees of any post-employment obligations. Review any agreements with the employee and make sure that he or she leaves with a copy. Ensure that a written record is kept, that the employee has been shown any agreements, and that a copy was provided to him or her.
- **Negotiate specific waivers.** If you learn that an employee may be taking a job that may technically constitute a violation of a restrictive covenant obligation, consider negotiating a limited waiver of those obligations. For example, if he or she is subject to a noncompete and wants to work for a competitor,

consider whether a customer restriction could provide you with adequate protection in the circumstances.

- **Inventory.** Arrange for the return of company property, including information that may be in electronic form on the employee's home computer.
- **Post-employment compensation.** If the departing employee's knowledge is particularly valuable, consider paying him or her not to work for a specified period of time.

3. Consistently Enforce Your Rights.

Employees will not take noncompetes and confidentiality agreements seriously if they observe that they are rarely if ever enforced. Similarly, if you never resist predatory hiring of your employees or misappropriation of trade secrets and other unfair competitive activities, you may be targeted as an easy mark.

Litigation, however, is a significant business decision. It is expensive and time consuming, and can be frustrating. Winning is never guaranteed, and counterclaims could subject you to possible liability. Consider all potential costs and benefits before initiating a lawsuit.

G. How Not To Get Sued - Some Practical Tips

Your company can be named as a co-defendant with a new recruit for claims including interference with contract, interference with prospective economic relationships, civil conspiracy, unfair competition, or misappropriation of trade secrets. If you lose, you may have to pay a substantial award of damages, or stay out of a market altogether for a period of time. Here are some practical tips for avoiding such a scenario.

1. Best Practices When Identifying Potential Recruits.

- The goal in hiring should be to gain good employees, not to appropriate trade secrets or to destroy the competition. Hiring a competitor's employees in order to gain competitive secrets or to deprive the competition of employees can lead to liability for "unfair competition" in a "raiding" case.
- Avoid making employees of specific competitors the sole or even primary focus of recruiting efforts. Instead, target the characteristics sought rather than the fact that employees worked at particular companies. This will avoid a mindset that unduly emphasizes acquiring information and personnel from competitors. The change in focus can also help avoid the generation of any documents that could be damag-

(continued next page)

Basic Noncompete Principles, Practical Tips and Best Practices... continued from previous page

ing in subsequent litigation brought by a competitor.

- Do not interview multiple employees from the same company at the same time. Document a legitimate business search for new recruits. An inference of predatory recruitment may arise if all of a company's recruiting resources were expended on a specific competitor, when similar recruits are available with other employers.

2. Best Practices Before and During the Interview Process.

- Routinely advise all applicants from the outset that you are interested in learning about the applicant and seeing whether there is a fit - not in learning a competitor's confidential information.
- Advise interviewers not to ask questions designed to elicit trade secrets, and to change the course of the interview if secrets appear to be presented.
- If the potential new employee is particularly important to his or her present employer, consider having more than one person present during the interview of the prospective hire. This will give you an added witness if you are sued by a competitor and added evidentiary effect at the time of trial.
- The interviewer should take steps to find out in *generic* terms what areas the employee has been working in that may raise trade-secrets concerns. For example, is the employee working on new technology that has not yet been publicly released, or is the employee working on any active bids? Without learning actual details, the hiring employer can begin considering whether some potential activities will have to be off limits, or even whether there may be an irreconcilable conflict.
- Satisfy yourself that nothing has been intentionally taken by the new employee from his or her former employer. Counsel the employee to return any materials later discovered.

3. Obtain and Analyze All Employment Contracts Before Extending an Offer.

- Ask applicants to provide copies of all signed agreements before a job offer goes out.
- Determine whether the restrictions appear to be appropriately tailored and enforceable, or whether they may be too long, too sweeping, or otherwise contrary to law. Some defenses to legal enforcement of such agreements include: lack of consideration; overly broad restrictions; no legitimate protectable interest; and equitable defenses *e.g.*, bad faith conduct, such as constructive discharge of the employee subject to the noncompete due to intolerable sexual harassment.
- Determine which state's law is likely to be applied to any restrictive covenants. Even if a particular state's law is identified and agreed to in the contract itself, if the employee worked in a different state from the specified law, "fundamental public policy" may lead a court to apply a different law.
- Require the new employee to represent, in writing, that the new position does not conflict with any agreements to which he or she may be a party, and that he or she will not use the old employer's confidential information.
- Alert new employees in writing that they may be terminated if their former employer files an action, if your company cannot afford or does not want to defend the claim.

Conclusion.

Employers can find themselves on either the plaintiff or defense side in cases involving proprietary information and trade secrets. Knowing the law and following basic "best practices" can help protect your company's valuable information and avoid litigation or, at a minimum, position you to the best possible advantage to protect your company's rights and business.

The Corporate Law Department Section Annual CLE

Hold the Date for the Corporate Counsel Institute on October 3,
2003, at the Washington State Convention & Trade Center.

USA PATRIOT Act and Terrorist Financing Regulations: Beware Your Compliance Obligations and Strict Liability

by Christopher A. Myers and Bradley B. Furber – Holland & Knight LLP

Many businesses, and their in-house or outside corporate counsel, have been surprised to learn that, since the September 11 attack on the World Trade Center, they have been enlisted in the government's campaign to halt terrorism. New regulations have been promulgated that require extensive and potentially expensive compliance measures across a broad swath of American businesses. Most corporate counsel and executives have heard of the USA PATRIOT Act and of President Bush's order freezing the assets of terrorists and blocking business relations with terrorists and their associates, but many remain in the dark about how those actions really affect them.

Two government actions continue to have a significant impact on how businesses conduct themselves in the post-September 11 world. First, on September 24, 2001, President Bush issued an Executive Order which created a list of persons, entities and groups believed to be connected with terrorism (the "Executive Order"). The President's Order bans *anyone* in the United States from conducting *any* business with *any* person, entity or group on the list. **This includes law firms, accounting firms and other service providers.** In addition, all reachable assets of those identified on this list have been frozen and any further dealings with them blocked by the President's Order. Any new or continued business relationship with a banned person or entity is a violation of the Executive Order and the statutes which authorized it, including the Trading with the Enemy Act. Violators are subject to substantial civil and criminal penalties. The Treasury Department and federal law enforcement authorities view violations of the Executive Order and related regulations as "strict liability" offenses. Even inadvertent violations will bring frozen assets and penalties.

Second, Congress passed the USA PATRIOT Act (the "Patriot Act") in October 2001. The PATRIOT Act was designed to cut off sources of financing for terrorists by strengthening the country's existing anti-money laundering laws. Those laws, including the Bank Secrecy Act ("BSA"), which have been on the books for years, were generally aimed at regulating the activities of "financial institutions." But until the PATRIOT Act, regulatory activities were focused on banks. The BSA actually contains a much broader definition of "financial institution," and the PATRIOT Act mandates regulation of all of them. Thus, the PATRIOT Act has caused a substantial impact on many U.S. businesses not heretofore

considered part of the anti-money laundering effort.

Awareness of the new requirements in many industries is significantly less than in traditional financial sectors. **Many businesses do not realize that they now fall within the definition of "financial institution," which includes: banks; commodities brokers; mutual funds; issuers or redeemers of travelers checks; operators of credit-card systems; telegraph companies; insurance companies; loan or finance companies; automobile, airplane and boat dealers; real estate brokers; persons or companies involved in real estate closings and settlements; securities broker dealers; investment companies; hedge funds; currency exchanges; money transmitters; pawnbrokers; travel agencies; dealers in precious metals, stones or jewels; and casinos. Other businesses may not be financial institutions, but are nevertheless covered by the Executive Order.** Whenever money could pass between a business and a person or entity on the government's terrorist list, the Executive Order applies.

Both the PATRIOT Act and the Executive Order will be enforced through a regime of substantial civil and criminal penalties, including the possibility of lengthy prison terms. Given the severity of criminal and civil sanctions for violations of the PATRIOT Act and the Executive Order, it is time that all businesses determine the extent to which they are covered by these new laws, and implement programs to comply with them.

So what should businesses do? The following sets forth some basic guidelines on what the law now requires, and what is likely to be required in the near future.

Presidential Order Blocking Transactions with Terrorists (Executive Order 13224)

Compliance with the Executive Order requires *all* businesses to ensure that they are not involved in *any* business with *any* person or entity suspected of terrorist involvement. When originally issued, the Order named twenty-seven individuals and entities, but it also specifically anticipated that additional persons and organizations would be added to the list.

The list, which is maintained by the Treasury Department's Office of Foreign Assets Control ("OFAC"), can be found at: <http://www.treas.gov/offices/enforcement/ofac/sanctions/terrorism.html>.

(continued next page)

USA PATRIOT Act and Terrorist Financing Regulations... continued from previous page

It has been updated numerous times since it was issued on September 24, 2001, and has been combined with the pre-existing "Specially Designated Nationals and Blocked Persons" list, often referred to as the "OFAC List." The OFAC List now is nearly one hundred pages long and consists of thousands of names, aliases, and "doing business as" designations. Many of the persons and entities on the OFAC List have common Arabic, Hispanic, or Anglo names, making it that much more difficult to determine whether a particular transaction is banned by the President's Order, or is merely a "false positive."

Regardless of the nature of the transaction, businesses, particularly those with some international component, must ensure that they are complying with the provisions of the Executive Order. This requirement is in effect now. There is no "grace" period, and companies cannot wait until they determine whether the new anti-money laundering requirements of the PATRIOT Act apply to them. Specifically, before entering into or continuing any financial relationship, businesses should check the identities of existing and potential clients, customers, vendors, employees and agents against the latest OFAC List.

The OFAC List can be checked manually, or it can be checked electronically through the use of software programs specially designed for the purpose. A manual check poses certain practical problems and risks that a good software program will address. One problem, the sheer size of the OFAC List – the number of names, aliases, and "doing business as" designations – means that a careful check will be very time-consuming. The task is further complicated by the fact that many of the names on the List are fairly common names, thus creating the possibility of a "false positive." These factors in combination greatly increase the risk of human error in making accurate manual checks. Further complicating the process is the fact that many of the names on the List include aliases which are not listed separately. And, while the current version of the OFAC List can be found at the OFAC website, it is updated so frequently that businesses choosing to conduct manual checks must constantly check the website to ensure they are using the latest version.

Software programs are now available that can search the OFAC List electronically. An electronic search yields nearly instant results and is far more cost-efficient than manual checks. A software program, however, also should include certain features if it is to be effective and ensure compliance. First, it must offer automatic updates whenever the OFAC List is amended, to make sure the most recent list is being searched. Second, it should immediately alert designated and appropriately trained

compliance personnel whenever there is a potential "match" between a customer, vendor, employee, etc. and a name on the List. Third, it should provide sufficient information about the "match" so that a reasonable and informed determination can be made about whether the "match" is accurate or is a "false positive." Fourth, it should block all further business with the matched person, group, or entity until it has been determined if the match is accurate. In addition, a good software program will instruct the user on what action to take when a match occurs. Finally, an effective system should include a case management system which documents searches and decisions made regarding potential matches in case of a government audit or investigation.

Holland & Knight's subsidiary, Corporate Integrity Services, in conjunction with its technology partner, DynCorp, has developed an integrated software-based compliance system which incorporates all of these features and more. The compliance solution is called *KnightGuardian*, and information is available through the authors.

Anti-Money Laundering Legislation: the USA PATRIOT Act

The September 11 terrorist attacks were supported and promoted by funds laundered through the U.S. financial system. Money laundering occurs when proceeds from illegal activities are converted into funds that appear to be legitimate and hide their true source or ownership. A sophisticated money laundering operation generally involves a series of transactions used to disguise the source of financial assets so that those assets can be used without compromising the criminals who control them. Illicit funds often begin in the form of cash, but can be converted into tainted money orders, wire transfers, bank drafts, checks, credit cards, and other payment instruments. Terrorist funding can also be laundered through other legitimate investment vehicles including insurance policies, securities, real estate, consumer products and many others.

The PATRIOT Act, passed in response to the September 11 attacks, focuses on and strengthens existing anti-money laundering laws, in part, through amendments to the Bank Secrecy Act. Prior to the PATRIOT Act, the BSA permitted the Treasury Department to require "financial institutions" to implement anti-money laundering compliance programs. "Financial institutions" is defined broadly under the BSA, and specifically includes many types of businesses that are not ordinarily thought of as financial institutions, as set forth above. Before September 11, the Treasury Department focused most of its regulatory attention on banks and exempted

(continued next page)

USA PATRIOT Act and Terrorist Financing Regulations... continued from previous page

most other BSA "financial institutions" from anti-money laundering requirements.

The PATRIOT Act removed discretion from the Treasury Department. It requires that "each financial institution shall establish anti-money laundering programs." These programs must include written policies and procedures; a designated Compliance Officer; employee training; and periodic auditing and monitoring. Further, among other provisions, the PATRIOT Act requires financial institutions to implement special account opening procedures and "Know Your Customer" due diligence. The PATRIOT Act further requires financial institutions to implement systems to check new accounts against government-provided lists of terrorists. Finally, the PATRIOT Act requires financial institutions to respond to government requests for information regarding possible business relationships with persons and entities suspected of, or being investigated for, terrorism, money laundering and other serious crimes.

Since enactment of the PATRIOT Act, the Treasury Department has been promulgating specific regulations for anti-money laundering programs for each of the different types of "financial institutions" identified in the Bank Secrecy Act. Most recently, in April of 2003, the Treasury issued a Notice of Proposed Rulemaking regarding anti-money laundering programs for "persons involved in real estate closings and settlements." A proposed rule is expected in the next few months.

In February of 2003, the Treasury Department began a new process by which financial institutions will be asked to provide information about persons under investigation by law-enforcement agencies. Under this new program, authorized by Section 314 of the PATRIOT Act, every other week Treasury's Financial Crimes Enforcement Network ("FinCEN"), via email or fax, sends out a list of persons under suspicion or investigation by law enforcement agencies. The financial institutions that receive this list must check all current accounts and business relationships to determine whether they are doing business with any of the persons on the list. If they are, they must report back to FinCEN, which, in turn, notifies the requesting law enforcement agency. Every two weeks a new list is sent out. Compliance with this requirement has proved to be cumbersome and time consuming for many financial institutions receiving the requests. As of May 2003, nearly 25,000 financial institutions were receiving the requests.

Finally, on May 9, 2003, the Treasury Department issued final regulations under Section 326 of the PATRIOT Act. These regulations require a broad range of financial institutions, including banks, credit unions, savings associations, securities broker dealers, mutual funds,

futures commission merchants, and introducing brokers to establish Customer Identification Programs ("CIPs"), which are intended to verify the identity of customers who open new accounts. The new regulations require affected companies to review certain identity verification documents and record information about them. Documents reflecting this information must be maintained for five years from the date the record is created. In addition, companies must verify the customer's identity such that the company has reasonable confidence that it knows the true identity of the customer. Finally, the CIPs must include a process for determining whether the customer appears on any government-provided list of suspected terrorists. FinCEN has not yet created or supplied a list of terrorists, but expects to do so in the future. This provision has caused some confusion among the regulated community, since, initially, it was believed to be related to Executive Order 13224 and the OFAC List. Both FinCEN and OFAC have made clear, however, that the two requirements are independent of each other, and the lack of a list of terrorists under Section 326 of the PATRIOT Act does not obviate the requirement to comply with the OFAC List and related regulations.

Conclusion

It is important to understand that *everyone* – all U.S. persons and businesses – must comply with the Executive Order, effective *now*. The obligation to check the OFAC List is completely separate from the issue of whether the Treasury Department will require a business to implement an anti-money laundering compliance program. Currently, all businesses in the U.S. must ensure that they are not involved in any transactions with a person or entity who appears on the OFAC List.

Although many businesses now defined as "financial institutions" typically are not thought of as targets for money laundering enterprises, the recent focus on terrorism financing has placed them in the same spotlight as banks, securities dealers, and other more traditional financial sectors. Increasingly, many types of business transactions and those involved in them are becoming the focus of international, as well as domestic scrutiny, as the methods and means of terrorism and money laundering are discovered and better understood. In the current climate, businesses need to take steps to ensure that they do not become unwitting participants in terrorist schemes. Failure to comply with the new requirements can result in severe civil or criminal sanctions. If a company ignores the requirements and, even inadvertently, engages in a transaction with a terrorist, criminal penalties could be imposed.

Speak Out!

Wanted: Lawyers to volunteer to speak to schools and community groups on a variety of topics. For more information about the WSBA speakers bureau call Amy O'Donnell at 206-727-8213.



Service Center... at your service!

800-945-WSBA or 206-443-WSBA
questions@wsba.org

We're here to serve you! The mission of the WSBA Service Center is to respond promptly to questions and requests for information from our members and the public.

Call us Monday through Friday, from 8:00 a.m. to 5:00 p.m., or e-mail us at *questions@wsba.org*.

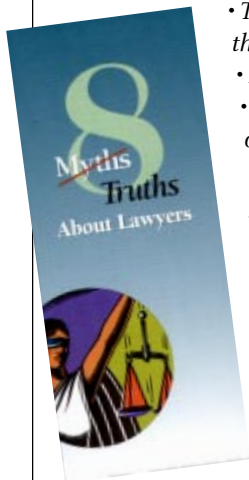
Assistance is only a phone call or an e-mail away.

8 Myths Truths About Lawyers

Help us stamp out some of those myths about lawyers! The *8 Myths Truths About Lawyers* brochure, developed by the Proud to Be a Lawyer Task Force, is available for purchase. The brochure tackles the following myths:

- *The United States has more lawyers than any other country.*
- *Lawyers are selfish and greedy.*
- *Lawyers stir up litigation for their own personal profit.*
- *Huge punitive damage awards are frequent and on the rise.*
- *The McDonald's verdict shows how foolish juries are.*
- *Lawyers who defend criminals are just promoting crime.*
- *When there's an accident, lawyers are among the first on the scene, soliciting business.*
- *The jury system is not worth keeping.*

The cost is \$35 per 100 (price includes shipping and handling).



Yes! I would like to order _____ packets @ \$35 per packet (100) \$ _____

If in Washington, please add WA state sales tax @8.8% \$ _____
Total \$ _____

check enclosed (payable to WSBA)

MasterCard Visa

No. _____ Exp. date _____

Name as it appears on card _____

Signature _____

Please send to:

Washington State Bar Association, Order Fulfillment
2101 Fourth Ave., Ste. 400, Seattle, WA 98121-2330

MasterCard and Visa orders may also be placed over the phone by calling the WSBA Service Center at 800-945-WSBA or 206-443-WSBA.

Name _____

Address _____

City _____ State _____ ZIP _____

WSBA office use only: 40800-COMM

date _____ check no. _____ amount _____

The WSBA is pleased to offer photo bar cards to active members. This is an option for those who are interested in having their photo on their card; original and replacement cards without photos are provided at no cost. Here's how it works:

- You can either e-mail an electronic photo in .bmp format or mail a hard-copy photo that we will scan. Photos can be any size.
- You may submit a black-and-white or color photo, however all photos will be printed in black and white.
- The cost is \$10 for cards created from electronic photos, and \$15 for cards created from hard-copy photos. Checks, MasterCard and Visa are accepted for payment.
- If you're mailing a hard-copy photo, please mail the photo with the completed order form and payment.
- If you're e-mailing an electronic photo, mail the completed order form with your payment. If paying by credit card, you may fax the order form.

If you have questions, please contact the WSBA Service Center at 800-945-WSBA, 206-443-WSBA or questions@wsba.org.

YES! I would like to order a photo bar card
(I am an active member).

Select one of the following:

- | | |
|---|----------------|
| <input type="checkbox"/> Photo submitted electronically | \$ 10.00 |
| (If in Washington, add WA state sales tax @ 8.8%.) | .88 |
| | Total \$ _____ |
| <input type="checkbox"/> Hard-copy photo enclosed | \$ 15.00 |
| (If in Washington, add WA state sales tax @ 8.8%.) | \$0 1.32 |
| | Total \$ _____ |

PHOTO BAR CARDS AVAILABLE

If submitting an electronic photo, please e-mail to amy@wsba.org. We recommend that you e-mail the photo the same day you send this form. If paying by credit card, you may fax this form to 206-727-8319. If submitting a hard-copy photo, be sure to write your name on the back and enclose it with this form. Your photo will be returned to you.

- check enclosed (payable to WSBA)
 MasterCard Visa

No. _____

Exp. date _____

Name as it appears on card _____

Signature _____

Please send to:

Member and Community Relations
Communications Division, WSBA
2101 Fourth Ave., Ste. 400
Seattle, WA 98121-2330

Name _____

Address _____

City _____ State ____ ZIP _____

WSBA office use only: 45060/LICMR

date _____ check no. _____ amount _____

CLE Credits for Pro Bono Work?

Limited License to Practice with No MCLE Requirements?

Yes, it's possible!

Regulation 103(g) of the Washington State Board of Continuing Legal Education allows WSBA members to earn up to six (6) hours of credit annually for providing pro bono direct representation under the auspices of a qualified legal services provider.

APR 8(e) creates a limited license status of Emeritus for attorneys otherwise retired from the practice of law, to practice pro bono legal services through a qualified legal services organization.

For further information contact Sharlene Steele, WSBA Access to Justice Liaison, at 206-727-8262 or sharlene@wsba.org.

This is a publication of a section of the Washington State Bar Association. All opinions and comments in this publication represent the views of the authors and do not necessarily have the endorsement of the Association nor its officers or agents.

WASHINGTON STATE BAR ASSOCIATION
Corporate Law Department Section
2101 Fourth Avenue, Ste. 400
Seattle, WA 98121-2330

Nonprofit Org.
U.S. Postage Paid
Seattle, WA
Permit No. 2204



Printed on recycled paper

Membership Enrollment Form

The officers and Executive Board of the Corporate Law Department Section invite you to join as a member. Seminars and newsletter reports are included in the benefits available to members. All Washington State Bar Association members are eligible.

- Please enroll me as an active member. Enclosed is a check for \$15 for annual dues.
- I am not a member of the Washington State Bar Association, but I want to receive your newsletter. My \$15 check is enclosed.

Current membership year: October 1, 2002-September 30, 2003

Name _____

Firm _____

Address _____

City _____

State _____ Zip _____

office use only

Send Enrollment Form and check to:
Corporate Law Department Section
Attn: Sections Liaison
Washington State Bar Association
2101 Fourth Avenue, Ste. 400
Seattle, WA 98121-2330

Date _____

Check # _____

Total \$ _____

**Corporate Law Department Section
Washington State Bar Association
EXECUTIVE COMMITTEE MEMBERS**

Officers & Committee Chairs

Jeff Christianson (Western Wireless Corporation), Chair	(425) 586-8013
Meredith Lehr Past Chair	(206) 232-3953
Eric Matson, Activities Committee, Treasurer	(425) 822-7191
Carol Haugen (Paine, Hamblen, Coffin Brooke & Miller), CLE	(509) 455-5178
Joel Summer (Miller Nash LLP), CLE	(425) 889-3415
Brian Lewis (Lewis Law Offices, PLLC) Newsletter	(206) 910-6574
Dave Anderson (Airborne Express), At-Large	(206) 830-1005
Wayne Michigami, (Starbucks) At-Large	(206) 318-5286
Karl Forsgaard, (Bendich, Stobaugh & Strong, P.C.) At-Large	(206) 622-3536