

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.
