

REAL ESTATE PROFESSIONALS:
ANTI-TERRORISM REGULATIONS
AFFECT YOU

February 8, 2005

Gregory Baldwin
Holland & Knight LLP
701 Brickell Avenue
Suite 3000
Miami, FL 33131
(305) 789-7745
greg.baldwin@hklaw.com

Christopher A. Myers
Holland & Knight LLP
1600 Tysons Blvd.
Suite 700
McLean, VA 22102
(703) 720-8038
chris.myers@hklaw.com

REAL ESTATE PROFESSIONALS: **ANTI-TERRORISM REGULATIONS AFFECT YOU**

Greg Baldwin and Chris Myers
Holland & Knight LLP

THE REAL ESTATE INDUSTRY HAS BEEN TARGETED BY MONEY LAUNDERERS, TERRORISTS AND THE FEDERAL GOVERNMENT.

► WHERE DO YOU STAND? ◀

► WHAT ARE THE RULES? ◀

► WHAT ARE THE ANSWERS? ◀

Recent media reports have identified real estate as a primary target for terrorists, money launderers and other criminals. Where the “bad guys” go, federal prosecutors and agents follow. Consider the following headlines:

- *Oxen Hill Development Has Ties to Terror* (Washington Post April 19, 2004)
- *Real Estate Was a Laundering Vehicle for Florida Mobsters, U.S. Says* (Money Laundering Alert May 2004)
- *Report Says Real Estate Among 'Most Significant' Laundering Tools* (Money Laundering Alert May 2004)
- *Comply with Executive Order on Terrorism to Avoid Stiff Penalties* (Commercial Lease Law Insider July 2004)
- *Fighting Terror with Brokers* (New York Daily News July 21, 2004)

These reports, along with numerous others, put companies and individuals involved in virtually every aspect of the real estate industry on notice that they have to be on the lookout for illegal activity tied to real estate in which they have an interest.

The Washington Post reported on April 19, 2004, that a Washington, D.C. area residential housing development is alleged by law enforcement authorities to have been an investment vehicle for the Palestinian group, Hamas, which has been declared by the government to be a terrorist organization. Investors in the project were identified as relatives of Osama bin Laden and others who have been named by the government as terrorists. Profits from the project were allegedly siphoned off to support terrorist activities.

In Miami, the Department of Justice recently indicted an alleged "Cuban-American mafia don" on numerous charges, including a variety of money laundering schemes. As part of its case, the government is seeking to forfeit more than \$1.5 billion

in assets, including twenty-nine separate bank accounts and fifty-one real estate properties. The properties include homes and condominium units.

Also in South Florida, the Immigration & Customs Enforcement agency ("ICE"), part of the Department of Homeland Security, has recently announced an enforcement initiative targeting money laundering and other related activities by corrupt political officials from other countries (Politically Exposed Persons, or "PEP's"). The ICE task force has already seized numerous bank accounts and real estate properties in which PEP's have invested using funds allegedly looted from their countries' treasuries. The ICE task force is expected to be expanded to other parts of the United States in the coming months.

In Orlando, Florida, the US Attorney's Office filed an indictment against one of the investors in a shopping center development. The indictment alleged various forms of immigration fraud related to smuggling illegal aliens from the Middle East into the United States, as well as money laundering related charges. As part of its case, *the government placed a freeze on the entire shopping center development*, threatening to stop the sale of one of the sections of the property. Only after an arrangement was made with the government to place the interest of the indicted individual in a blocked account, was the transaction allowed to go forward.

In its July, 2004, the Commercial Lease Law Insider (CLLI) reported that commercial real estate owners and managers risked stiff fines and potential criminal charges if they did not take steps to insure that their tenants, employees, contractors, suppliers and anyone else involved in a property were not on a government list of terrorists and other criminals. Similarly, the New York Daily News, on July 21, 2004, described steps that commercial real estate brokers were taking to make sure that they were not leasing space to terrorists and other prohibited parties. These articles further reported that many in the industry were unaware of these obligations.

These are just a few of the many examples in which law enforcement authorities have alleged that various types of commercial and residential real estate projects have been used as vehicles for terrorist financing or laundering of the proceeds of other criminal activities. What is the basis for these enforcement activities, and what can people and companies involved in the real estate industry do to protect themselves?

Three Enforcement/Regulatory Regimes Related to Terrorism and Money Laundering Directly Affect the Real Estate Industry

Three separate, but related regulatory regimes, used by the government to fight terrorism and money laundering, directly impact the real estate industry. Two are in effect now, and expose real estate entities to significant risk. The third has temporarily exempted real estate organizations, but new regulations are expected soon.

- ***The Money Laundering Control Act*** is a criminal statute and is in effect now.

- ***The USA PATRIOT Act and Bank Secrecy Act*** require certain anti-money laundering compliance activities will result in regulations directly affecting the real estate industry in a matter of months.
- ***The OFAC List*** is issued by the Treasury Department's Office of Foreign Assets Control ("OFAC") and contains the names of thousands of "Specially Designated Nationals" ("SDNs"). The "OFAC List," also known as the "SDN List") is in effect now. It has significant civil and criminal penalties.

The Money Laundering Control Act

The Money Laundering Control Act (MLCA) imposes severe criminal penalties on individuals or companies who are "knowingly" involved in a transaction involving the proceeds of a broad variety of criminal activities. The penalties include jail terms of up to 20 years and substantial fines of either \$500,000 or twice the value of the property involved, whichever is *greater*.

Generally, the MLCA makes it illegal for any person or business that "knows" money or property is derived from "some" illegal activity to engage in a financial transaction involving that money or property if the money or property did, in fact, come from a "specified unlawful activity."

Knowledge that the money or property came from "some" illegal activity can be established if the party charged is found to have deliberately ignored facts or circumstances which would raise questions for a reasonable person about the source of the money or property. This is called "willful blindness" and comes dangerously close to a "should have known" standard. If a person or business is found to have been "willfully blind" to the illegal source of money or property, many courts will assume that the person or business *actually knew* that the source was illegal activity.

Knowledge that the money or property came from "some" illegal activity means that the money or property was believed to have come from any violation of *federal* criminal law, any violation of a *state* criminal law, or any violation of a *foreign* criminal law. The person involved in the transaction does not have to correctly identify the true criminal source of the money or property. Even if the person is wrong about the illegal source, knowledge or belief that it comes from *any* illegal act is sufficient.

A "specified unlawful activity" includes virtually any violation of federal law. It also includes violations of certain *foreign* laws, including fraud by or against a foreign bank, illegal drug dealing, murder or other crimes of violence, and public corruption.

While there is no rule that says a business may rely on the anti-money laundering efforts of another business, it is usually a good idea to include in a contract certain terms, conditions, representations and warranties that require the person or business you are contracting with to perform basic anti-money laundering procedures.

The MLCA is in effect *now*, and it applies to every person and business in the U.S. as well as to persons or businesses *outside* the U.S. that is involved in the transaction (if even a part of the transaction comes into the U.S.).

In light of the targeting of real estate by money launderers, terrorists and other criminals, every person and business involved in the real estate industry should be on guard.

The USA PATRIOT Act/Bank Secrecy Act

With respect to anti-money laundering requirements, the USA PATRIOT Act essentially amends the federal “Bank Secrecy Act,” which was originally passed in 1970. The Bank Secrecy Act, or “BSA,” is the federal statute that grants to the U.S. Treasury Department the authority to issue regulations to various types of businesses requiring certain anti-money laundering (“AML”) actions. The BSA has established twenty-seven classes of “financial institutions” that are potentially subject to Treasury Department anti-money laundering regulation. Among these “financial institutions” are banks, loan or finance companies, investment companies and “persons involved in real estate closings and settlements.” Under the USA PATRIOT Act, all twenty-four classes of “financial institution” must implement AML compliance programs.

The Treasury Department is empowered to require real estate entities to establish formal written AML programs, appoint AML compliance officers, educate employees about AML procedures, and periodically check the AML program to ensure it is working. AML requirements can also include procedures for obtaining documentation of the identity of customers and checking customers against government lists of terrorists. AML rules can also require that regulated businesses report “suspicious activity” to the government. AML programs must, as a practical matter, include “Know Your Customer” (or “KYC”) procedures to enable employees and businesses to know who their customers are and to identify money laundering and other “suspicious activity.”

Three of the four categories of “financial institution” listed above (loan or finance companies, investment companies and “persons involved in real estate closings and settlements”) have not yet been specifically defined by Treasury. Therefore, it is not yet clear exactly which businesses involved in the real estate industry will be subject to AML regulation. Draft regulations implementing the AML requirements are currently under development by Treasury and are expected to be published in the next several months. However, because of the current applicability of the criminal Money Laundering Control Act and OFAC List regulations, and because it is clear to law enforcement authorities that real estate is a prime target for money launderers, it is very advisable for companies involved in the real estate industry to establish AML programs as soon as possible.

While there is no rule that says a business may rely on the AML or KYC due diligence of another business, it is, again, usually a good idea to include in a contract certain terms, conditions, representations and warranties that require the person or business you are contracting with to perform these basic functions.

OFAC: Prohibited Persons, Businesses and Groups

The Office of Foreign Assets Control publishes a list of persons, businesses and groups that it is illegal for *all* U.S. individuals and businesses to engage in *any* of kind of transaction with. In addition, in response to the September 11, 2001, terrorist attacks, President Bush issued Executive Order 13224 prohibiting *all* U.S. individuals and businesses from engaging in *any* of kind of transaction with persons, groups or entities designated as terrorists or as their supporters or associates. A combined list of “Specially Designated Nationals” (“SDN’s”), consisting of “drug kingpins,” terrorists and others considered a danger to the United States, is the result. Known variously as the “OFAC List,” the “SDN List” and the “OFAC SDN List,” it now contains about 5,000 names and is about 140 pages long. No individual or business in the U.S., or the foreign subsidiaries of U.S. companies, may conduct any kind of business with anyone on the List. The List is frequently modified (since 2001, on an average of over 30 times per year; more than 15 times as of May 2004 alone), and companies are expected to keep track of all changes. The “OFAC List” can be accessed at OFAC’s website, <http://www.treas.gov/offices/eotffc/ofac/sdn/index.html>.

Compliance with this prohibition is enforced through OFAC. OFAC, in guidance recently released, has specifically identified real estate as a target for enforcement and special attention.

"There is an absolute prohibition against engaging in transaction with individuals or entities on OFAC's list of Specially Designated Nationals and Blocked Persons (the "SDN" List"), named parties owned or controlled by, or acting for or on behalf of, targeted governments or groups such as international narcotics traffickers or terrorists."

Criminal violations of the OFAC regulations "*can result in corporate and personal fines of up to \$1 million per count and, in the case of individuals, a maximum of 10 to 12 years in jail per count.*" Civil fines can range from \$11,000 to \$275,000 per count. National and international law enforcement agencies have specifically identified real estate as a prime target for terrorists and money launderers.

OFAC regulations do not expressly permit businesses to delegate their OFAC responsibilities to others, and OFAC officials have stated that such delegation does not relieve a party from liability for a violation. Nevertheless, it is usually a good idea to include in a contract certain terms, conditions, representations and warranties that require the person or business you are contracting with to perform this basic activity.

The OFAC SDN List: What is Required?

The OFAC rules and regulations are all-encompassing and extremely broad. They literally prohibit *all* persons and businesses from engaging in *any* transaction or providing *any* financial service or other assistance to a person, group, business entity or

country on the OFAC SDN List. The only way for businesses to protect themselves from running afoul of this sweeping prohibition is to check the name of every customer, client, vendor, employee and associate against the OFAC SDN List for every transaction.

The OFAC prohibitions, read literally, mean that, for example, every drug store in the U.S. should check the name of every customer at the cash register in order to ensure that it is not selling aspirin to a terrorist. Obviously, this is neither practical or commercially feasible. OFAC, however, has refused to identify a “*de minimus*” amount below which they will not enforce. They reserve the right to evaluate situations on a case-by-case basis, and have stated that even inadvertent violations will be considered strict liability offenses. So where does one draw the line? What transactions really need to be checked? And how deeply must one check? Does checking against the OFAC SDN List require that a business must check its client’s clients?

Given the broad language of the federal statutes involved, the OFAC regulations provide very little specific guidance on these questions. Based upon our experience dealing with OFAC and other anti-terrorism enforcement regimes, however, we suggest the following general guidelines.

- The fastest and most efficient way to check names on the OFAC SDN List is through a reliable computer software system that is integrated into carefully designed compliance procedures.
- Check every name you can get – once on a computer system, extra names can be checked with little additional time or cost.
- Do not check only certain types (or stereotypes) of persons or businesses; terrorists and other prohibited parties come from all countries, are members of every religious group, and include all races, cultures and ethnicities.
- Document your activities, so that if questions later arise, you can easily retrieve information that supports your compliance activities.
- If you are a Lender, a Purchaser or a Seller, or are in a secondary market transaction, the ask for and check the name of the:
 - ~ seller,
 - ~ the seller’s guarantor or indemnitor
 - ~ the seller’s chief beneficial owners*
 - ~ the borrower
 - ~ the borrower’s guarantor or indemnitor
 - ~ the borrower’s chief beneficial owners*
 - ~ you need not check the beneficial owners of the owners of the seller¹ or borrower, but if you have those names, check them

¹ In a recent discussion, a member of the OFAC General Counsel's Office pointed out that persons or entities several levels removed from the direct party involved in a transaction could be prohibited parties, and thus covered by OFAC regulations. He stressed that companies must implement and follow "reasonable" procedures. The cut-off points outlined here could be viewed as reasonable in most circumstances, he said, but if information came to light in the course of normal due diligence that pointed

- If you are involved in a commercial real estate deal, in addition to the above (as applicable) the ask for and check the name of the:
 - ~ the property manager
 - ~ every existing tenant, if you're the buyer
 - ~ ensure that the property manager or some reliable party checks the name of every future tenant (including their chief beneficial owners)
- If you are involved in a joint venture to own or develop commercial real estate, check the name of :
 - ~ every partner in the joint venture
 - ~ the chief beneficial owners of each partner*
 - ~ you need not check the beneficial owners of the owner of each partner, but if you have those names, check them
- If you are sponsoring a Fund involved in owning or developing commercial real estate, check the name of :
 - ~ every investor
 - ~ the chief beneficial owners of each investor*
 - ~ you need not check the beneficial owners of the owner of each investor, but if you have those names, check them

* We suggest that a chief beneficial owner may be reasonably defined as a person or entity that holds 25% or more of the ownership or voting rights of a business. While this 25% figure is not part of the OFAC regulations, it is based upon current Treasury Department anti-money laundering regulations that require banks and other institutions in the U.S. to know (and keep a record of) the "owners" of foreign banks for which they maintain correspondent accounts. *See* 31 C.F.R. §§ 103.75, 103.77.

If you get a "hit," or potential match between the OFAC SDN List and a name you're checking:

- ~ use all identifying information on the OFAC SDN List to determine whether the person or entity you are checking is really the person or entity on the List (if necessary, get additional identifying data from the person or entity you are checking)
- ~ call your counsel or the OFAC "hot line" for assistance if necessary
- ~ freeze and segregate any assets of the confirmed matched person, group or entity in your possession

to the possibility that someone on the OFAC List was involved in a transaction, additional checking might be required.

- ~ notify OFAC of the true matches (using specially designed forms issues by OFAC), and consider notifying the FBI; follow instructions from OFAC

Compliance With Anti-Terrorism Regulations

Holland & Knight has extensive experience in advising clients on all anti-terrorism and anti-money laundering issues, including the design and implementation of compliance programs and procedures to help them avoid or correct problems. In combination with our real estate lawyers, we are positioned to develop cost-effective solutions for companies in the real estate industry.

In addition, through our subsidiary, Corporate Integrity Services, we have developed a software tool to help companies comply with OFAC and other prohibited parties regulations. The solution is called "KnightGUARDIAN" and is available in a variety of formats to best fit with the business and compliance processes of our clients.

KnightGUARDIAN was designed with the advice of members of our White Collar and Corporate Compliance team, who are Certified Anti-Money Laundering Specialists. It includes features which those lawyers would want to have available in the event a client was being investigated or charged with violations of OFAC regulations or the anti-money laundering laws.

For further information KnightGUARDIAN, the Money Laundering Control Act, the PATRIOT Act or AML and KYC compliance in general, contact Holland & Knight partners Christopher Myers (703) 720-8038 (chris.myers@hklaw.com) or Greg Baldwin (305 789 7745) (greg.baldwin@hklaw.com).

2530058_v1