

Federal Anti-Terrorism Laws And Law Firm Clients

by Trip Mackintosh, Lizbeth Rodriguez, and Stephen Masciocchi

This column is sponsored by the CBA Ethics Committee. Articles published in this column do not necessarily reflect the views of the Committee and may be those only of the individual authors.

Column Editor:

Susan Bernhardt, Denver, of Netzorg, McKeever, Koclanes & Bernhardt LLP—(303) 864-1000, sbernhardt@nmkb.com

About The Authors:



This month's article was written by Trip Mackintosh, a partner at Holland & Hart, LLP, specializing in federal regulation of international business and white-collar defense; Lizbeth Rodriguez, an associate at Holland & Hart, LLP, practicing domestic and international business law; and Stephen Masciocchi, a partner at Holland & Hart, LLP, where he is chair of the firm's Ethics and Conflicts Committee. The authors may be reached at (303) 295-8000.

Federal anti-terrorism laws include regulations that restrict attorneys from doing business with persons or entities on various "blocked persons" lists and carry stiff penalties for noncompliance. Law firms should take measures to ensure compliance with these regulations, including screening client names against the lists and obtaining applicable licenses before assisting listed clients.

Since the events of September 11, 2001, Colorado lawyers have faced a number of challenges as laws affecting travel, civil liberties, and international commerce have changed. Unnoticed by many in the Bar are laws that impose obligations on businesses and individuals, including lawyers, to avoid unauthorized dealings with clients whose names appear on federal "blocked persons" lists and the potential liability for noncompliance with those laws. This article outlines some of these principal obligations. It also suggests measures attorneys can take to prevent inadvertent violations of federal export regulations.

Homeland Security, Export Regulations, and The Practice of Law

At the core of the U.S. Department of Homeland Security ("Homeland Security") anti-terrorism efforts are controls designed to deprive terrorist entities of funds and technology. These "anti-terrorism controls" sometimes are referred to as "non-proliferation initiatives," inasmuch as their goal is to impede the proliferation of munitions or weapons-applicable technologies and the funds required for their application. These non-proliferation controls affect with whom U.S. persons can do business, what sort of business can be conducted, and how that business may be pursued. All of these laws impact privacy and security concerns in today's society.

To be effective, anti-terrorism controls must reach the street level of commerce—that is, from the largest company to the smallest. Law firms conducting international business or doing business with foreign persons naturally are subject to these federal regulatory controls. To prevent an inadvertent violation of anti-terrorism controls and face the risk of potential penalties, law firms, as with any other U.S. businesses, need to be aware of these regulations and implement measures to prevent potential violations.

Together with other Homeland Security efforts and related foreign policy initiatives, U.S. export controls, which affect the "who," "what," and "how" of international business, have a broad and extra-territorial reach. As discussed below, penalties for noncompliance are severe, reflecting the national security imperative behind the regulations. The underlying national security imperative and possible penalties emphasize the need for compliance.

Unfortunately, the anti-terrorism laws render illegal otherwise legal commercial conduct, thereby making compliance difficult. To complicate matters, these laws are enforced simultaneously by a number of agencies. Often the agencies have seemingly conflicting regulations. Further, a particular agency's rules are complicated to the degree that the U.S. Bureau of Immigration and Customs Enforcement ("U.S. Customs") officials charged with their enforcement

can inadvertently make mistakes in applying them.

Laws Governing Business Relationships

Federal anti-terrorism controls capture virtually every aspect of international commerce. For example, these controls reach, but are not limited to:

- Financial transactions involving anything of value
- The provision of services of any sort, including legal services
- Dealership agreements
- Distribution arrangements
- Stock transfers
- Exports of know-how
- Technology transfers
- Employment of non-U.S. staff
- Exports of goods out of the United States
- Mere proposals for certain exports.¹

The federal government's most sweeping anti-proliferation initiatives involve restrictions on the entities or persons with whom U.S. persons may conduct business. Violations of these restrictions present the easiest prosecutions, because they require only a demonstration that business took place with a prohibited party. Complying with these laws, however, may prove difficult without a clear understanding of the regulations issued by several U.S. departments which, at times, have overlapping jurisdiction.

The U.S. Departments of Commerce, Treasury, and State issue different lists of parties with whom U.S. parties are prohibited from conducting business. Doing business—which includes providing legal services—with parties included on any of those lists may result in criminal and administrative penalties for a law firm. A number of exceptions, however, apply to certain transactions with certain parties. Consulting the regulations themselves and a specialist in the field is recommended because the exceptions often are not published. Following is a brief summary of these list-based anti-terrorism restrictions. These prohibited-party lists are online, and the Appendix to this article provides a listing of the websites.

Treasury Department Regulations

The Department of Treasury, through the Office of Foreign Assets Control ("OFAC"), regulates and implements controls brought under the Trading with the Enemy Act, as amended;² the Interna-

tional Economic Emergency Powers Act ("IEEPA");³ and several other laws directed at specific countries.⁴ OFAC prohibits or restricts trade with certain countries and an ever-growing directory of individuals and companies.⁵

Specially Designated Nationals List: OFAC maintains the primary list of concern for U.S. companies doing business with foreign parties: the Specially Designated Nationals List ("SDN List").⁶ The SDN List includes terrorists, drug traffickers, and persons or companies acting on behalf of embargoed countries, territories, and drug traffickers. When the U.S. government determines that a party is a buyer for an embargoed country, the U.S. government "specially designates" this party as a national of that country.

Inclusion on the SDN List can occur at any time, even during the pendency of a transaction with a U.S. company or while a party is a client of a U.S. law firm. Absent provisions in the OFAC regulations,⁷ or a license from OFAC, U.S. persons (including lawyers) and companies (including law firms) are not allowed to conduct business with individuals or entities included on the SDN List. License applications to conduct business with a party included on the SDN List may be filed with OFAC. As of August 10, 2004, the list ran more than 143 pages, with an additional forty-seven pages of changes since January 1, 2004.⁸

Specially Designated Global Terrorists: The SDN List also includes Specially Designated Global Terrorists ("SDGT"). As the federal government identifies individuals or companies considered to be "associated with" terrorist-supporting entities, these individuals and companies can be designated as SDGT and added to the SDN List. U.S. persons, companies, and firms are prohibited from conducting business with parties designated as SDGT.

It is important to note that individuals or companies designated as SDGT or otherwise listed on the SDN List could be international trading partners of a client, with which a law firm or its client has conducted business legally for years.⁹ Thus, law firms and their clients alike need to be aware of this fact and conduct careful screening of their international trading partners and other foreign persons and entities with which they conduct business.

Sanctions and Embargoes: The U.S. government has imposed sanctions and maintains embargoes against a number of countries around the world. Each embargo varies, depending on the country in

question, but generally an embargo prohibits conducting business with the governments, companies, and nationals of the targeted country. OFAC administers and implements the U.S. embargoes. Currently, the U.S. maintains comprehensive economic embargoes against Cuba, Iran, Syria, and the Sudan.¹⁰

The embargo rules are ambiguous in many respects. For example, a U.S.-owned subsidiary outside the United States can deal directly with Syria, Iran, or other sanctioned countries, as long as no U.S. person facilitates or approves the transaction. This is true even if the foreign subsidiary is directly controlled by the U.S. parent, provided that no U.S. person participates in the transaction. However, the addition of a U.S. lawyer in the transaction would mean that the exception would no longer apply and that the lawyer may face penalties for violation of the regulations.¹¹

Department of Commerce Regulations

The Department of Commerce, through the Bureau of Industry and Security ("BIS"), also prohibits conducting business with certain parties. BIS aims its prohibitions at: (1) parties who have violated U.S. export control laws—for example, by receiving illegally exported technology; and (2) entities engaged in proliferation activities—for example, government-owned facilities in the People's Republic of China or Pakistan, private concerns identified as buyers for proliferation projects, and hundreds of other entities world-wide.

Denied Persons List: BIS maintains the Denied Persons List ("DPL").¹² "Denied persons" include persons and companies prohibited from receiving U.S. products because they have violated U.S. export control laws. U.S. parties cannot conduct most business with these parties absent specific authorization from BIS. These activities include, by way of example, financing, services of any sort (including legal services), shipping, and management functions that could assist with an export transaction.¹³

Entity List: BIS also maintains a list of entities engaged in proliferation activities ("Entity List").¹⁴ The Entity List includes end-users that have been determined to present an unacceptable risk of diversion to developing "weapons of mass destruction" or missiles used to deliver those weapons. U.S. businesses cannot deal with these parties absent specific authorization from BIS. License requests to

deal with persons and entities on either the DPL or the Entity List must be filed with BIS.¹⁵

Unverified List: In addition to the DPL and the Entity List, BIS also maintains a list of recipients of U.S. exports who have (for one reason or another) not allowed the United States to verify that they are using the technology in the manner reported (“Unverified List”).¹⁶ The Unverified List includes the name and country of origin of foreign persons who in the past were parties to a transaction to which the Department of Commerce could not conduct a pre-license check or a post-shipment verification for reasons outside of the U.S. government’s control. Although trade with these parties is *not* prohibited, trading with them absent some demonstrable assurance of non-proliferation leaves the U.S. party open to the allegation that it knowingly disregarded a proliferation risk and, consequently, is at risk of potential penalties.

State Department Regulations: Debarred Parties List

Although the Treasury and Department of Commerce prohibitions apply to any trade with denied or prohibited parties, the State Department is more limited in its prohibitions. As the regulator of munitions exports, the State Department maintains a list of “debarred” parties (“Debarred Parties List”)—that is, those who cannot receive exports of U.S.-origin munitions.¹⁷ The term “munitions” is not limited to military items. The term includes any technology that has been specifically designed or modified for military application. As with the Treasury and Department of Commerce list-specific prohibitions, any effort to engage in a transaction with a debarred party may result in criminal or administrative sanctions.¹⁸

Penalties

Conducting international business with a party on any of the lists described above, or mere participation in a transaction with them, can result in criminal and administrative charges. Depending on the circumstances, mere proposals to conduct business or misdirected efforts at compliance also can result in criminal or administrative charges. In some circumstances, structuring a transaction involving a prohibited party in a manner that appears to comply with these restrictions can be interpreted as an attempt at evasion.

Even if an attorney is unaware of the circumstances of the transactions in which he or she is involved, not checking the lists can result in challenges to the attorney-client privilege, thereby creating problems for the attorney and the client. The government has been quick to assert the crime-fraud exception to the privilege if it appears the attorney was used (even unwittingly) in a transaction with a denied or prohibited party. Lack of knowledge is not a defense, and failure to comply may result not only in penalties for violating these laws but in losing the attorney-client privilege.

Penalties may be criminal, civil, or both. For example, willful violations of the Department of Treasury regulations can produce fines of \$50,000.¹⁹ Violations of the Cuban embargo sanctions can produce fines of \$1 million (for a corporation) and \$100,000 (for an individual).²⁰ Individuals also may be imprisoned for not more than ten years for violations of the Department of Treasury regulations.²¹

Civil penalties of not more than \$11,000 may be imposed for violations of most of the Department of Treasury embargoes, such as the Iranian sanctions.²² Civil penalties of not more than \$55,000 per violation also may be imposed for violations of the Department of Treasury regulations regarding Cuba.²³

Willful violations of the Department of Commerce regulations can lead to: (1) criminal penalties of up to ten years in prison; or (2) fines of five times the value of the export up to \$1 million (for a corporation) or \$250,000 (for an individual), or both.²⁴ Export violations under the Department of Commerce rules can result in civil penalties of up to \$100,000 and denial of export privileges.²⁵

Importantly, under all of these regulatory regimes, each export or transaction can produce multiple violations. The penalties are not per “transaction,” leaving open the possibility that one export transaction can produce multiple violations and rapidly increase an exporter’s liability. The regulators employ the principles of “parsing and stacking” to multiply the number of potential violations.

Violation of Ethical Rules

Depending on the circumstances, violations of export regulations also may result in violations of the Colorado Rules of Professional Conduct (“Colorado Rules” or “Colo.RPC.”). Lawyers who take on blocked persons or entities as clients without screening them or without complying

with the applicable regulations could conceivably run afoul of the following Colorado Rules:

- Colo.RPC 1.1 (concerning competence)
- Colo.RPC 1.2(e) (requiring consultations with clients concerning limitations on the lawyer’s conduct)
- Colo.RPC 1.7(b) (concerning conflicts created by a lawyer’s own interests)
- Colo.RPC 8.4(a) (providing that it constitutes misconduct to violate a rule or assist another in doing so).

Likewise, lawyers who commit criminal violations of export regulations could be subject to discipline under the Colorado Rules. These relevant rules include:

- Colo.RPC 8.4(b) (committing a criminal act that reflects adversely on a lawyer’s fitness)
- Colo.RPC 8.4(d) (conduct prejudicial to the administration of justice)
- Colo.RPC 8.4(h) (other conduct that adversely reflects on a lawyer’s fitness).

Law Firm Procedures to Prevent Violations

The regulations and potential penalties discussed above have important implications for any law firm that engages in international transactions or does business with foreign parties. Although no national or statewide practice standards have been developed, issues that firms should consider include: (1) identifying listed clients; (2) assisting clients with removal from the lists, which may involve obtaining agency licenses; and (3) dealing with agency investigations.

Implementing a Compliance System

The most effective way for a law firm to prevent potential violations of the export regulations discussed above is to implement a comprehensive internal compliance system. Such a system should ensure that law firms fulfill their part in screening illicit transfers of technology and funds. Moreover, attorneys should advise any client who may be impacted by these controls of the existence of the lists of prohibited parties and the potential consequences of doing business with a prohibited party.

Law firms conducting business with foreign parties or involved in international transactions should establish a system to screen their current and potential clients against the prohibited-party lists,

adding this task to their regular process of screening new matters for conflicts of interest. The two most important lists for client screening purposes are the SDN List and DPL. These lists cover a broad range of both listed individuals/entities and prohibited activities. Most law firms will run little risk from failing to screen client names against the remaining lists unless they have clients who deal directly in munitions or are engaged in proliferation activities.

After clients have been screened, firms must exercise continued vigilance, because the lists are not fixed. As a result of ongoing investigative activities of federal agencies, parties can be added to the lists at any time. Therefore, a well-designed screening system will include a process to periodically re-screen current clients against the updated lists. Because the lists are available on the Internet, re-screening existing customers is not a cumbersome process. There is no set standard regarding how often the screens need to be conducted, so each law firm will have to use its business discretion regarding this screening process.

Removing Names from Lists

If a current or potential client appears on the list, it is possible that the client's name was added in error or that other circumstances would warrant removal from the list. Commentators and civil libertarians have assailed prohibited-party lists as being inaccurate, over-inclusive, and violative of constitutional rights. They have further complained that the administrative procedures available for removing names from the lists are inadequate and provide for limited judicial review.²⁶ The process for removing a name from a list depends on the governmental agency's procedures, but it would probably require the filing of an administrative appeal with the applicable governmental agency.²⁷

In the event that a client's name appears on a list in error, a law firm should proceed with caution in assisting the client in requesting de-listing. Once a client is listed, the firm may have to receive a license from the Treasury, Commerce, or State Department, as applicable, prior to providing any further services to the client (including assisting in getting a client's name removed from a list). This li-

censing requirement will vary depending on the embargo regime or other grounds for listing of the client.

Investigation Considerations

In the more serious event that a client or law firm is caught in an investigation premised on any of the regulations discussed in this article, the situation calls for a somewhat specialized defense protocol. In these instances, the client or firm should retain experienced counsel both to handle the traditional criminal defense and to make changes in their compliance procedures so as to demonstrate proper remediation and compliance efforts. A well-designed compliance program, including recordkeeping and screening efforts, could be considered a mitigating factor in the event of a violation.

Conclusion

The "war on terror" has domestic ramifications that can reach into a law firm's client list. The best counter-measure is a comprehensive compliance program that screens clients and ensures that the firm and its clients are well educated about

these issues. A well-designed screening system will help a law firm avoid potential violations of regulatory controls for inadvertently conducting business with a prohibited party. Prevention is the most effective way to ensure compliance and avoid being subject to a federal investigation.

NOTES

1. See generally 15 C.F.R. §§ 774 *et seq.* (2004); 22 C.F.R. §§ 120 *et seq.* (2004).
2. 40 Stat. 411 (2004).
3. 50 U.S.C. §§ 1701 *et seq.* (2004).
4. See, e.g., The Cuban Democracy Act of 1992, 22 U.S.C. §§ 6004 *et seq.* (1992).
5. See generally 31 C.F.R. §§ 500 *et seq.* (2003).
6. The SDN List can be found at <http://www.treas.gov/offices/enforcement/ofac/sdn>.
7. 31 C.F.R. §§ 500 *et seq.* (2004).

8. SDN List, *supra*, note 6. Changes to the SDN List are also on the website.

9. See 31 C.F.R. §§ 594 *et seq.* (2003).

10. See 31 C.F.R. §§ 515 *et seq.* (2003); 31 C.F.R. §§ 550 *et seq.* (2003); 31 C.F.R. §§ 560 *et seq.* (2003); Exec. Order No. 13338, 69 Fed. Reg. 26751 (2004). For a summary of the current sanctions, see <http://www.treas.gov/offices/enforcement/ofac/sanctions>.

11. A general overview of the OFAC rules can be found on the Department of Treasury website at <http://www.treas.gov/offices/enforcement/ofac>. The OFAC regulations are codified at 31 C.F.R. §§ 500 through 599.

12. The DPL is found at <http://www.bis.doc.gov/dpl/Default.shtm>.

13. See generally 15 C.F.R. §§ 730-774 (2003).

14. The Entity List is found at <http://www.bis.doc.gov/Entities/Default.htm>.

15. For information on general licensing requirements, see <http://www.bis.doc.gov/licensing/index.htm>.

16. The Unverified List can be found at http://www.bis.doc.gov/Enforcement/UnverifiedList/unverified_parties.html.

17. The Debarred Parties List can be found at <http://pmdtc.org/debar059.htm>.

18. See 22 C.F.R. § 127.7 (2004).

19. 31 C.F.R. § 535.701 (2003).

20. 31 C.F.R. § 515.701 (2003).

21. 31 C.F.R. § 500.701 (2003).

22. 31 C.F.R. § 535.701 (2003).

23. 31 C.F.R. § 500.701 (2003).

24. 15 C.F.R. § 764.3 (2003).

25. *Id.*

26. See, e.g., Fitzgerald, "Managing 'Smart Sanctions' Against Terrorism Wisely," 36 *New England L.Rev.* 957, 974-75 (2002); Liptak, "A.C.L.U. Board is Split over Sanctions," *N.Y. Times* (July 31, 2004) at A1; Liptak, "A.C.L.U. to Withdraw from Charity Drive," *N.Y. Times* (Aug. 31, 2004) at A23.

27. See, e.g., 22 C.F.R. § 128.13 (2004). ■

APPENDIX: Online Lists of Prohibited Persons and Entities

List	Responsible Agency	Website
<i>Specially Designated Nationals and Blocked Persons ("SDN")</i> List: Terrorists, drug traffickers, and persons or companies acting on behalf of embargoed countries, territories, and drug traffickers	Department of Treasury, Through the Office of Foreign Assets Control ("OFAC")	http://www.treas.gov/offices/enforcement/ofac/sdn
<i>Denied Persons List ("DPL"):</i> Persons and companies prohibited from receiving U.S. products because they have violated U.S. export control laws	Department of Commerce, Through Bureau of Industry and Security ("BIS")	http://www.bis.doc.gov/dpl/Default.shtm
<i>Entity List:</i> Entities engaged in proliferation activities	Department of Commerce, Through BIS	http://www.bis.doc.gov/Entities/Default.htm
<i>Unverified List:</i> Recipients of U.S. exports who have not allowed the United States to verify that they are using the technology in the manner reported	Department of Commerce, Through BIS	http://www.bis.doc.gov/Enforcement/UnverifiedList/unverified_parties.html
<i>Debarred Parties List:</i> Those who cannot receive exports of U.S.-origin munitions	State Department, Through the Directorate of Defense Trade Controls	http://pmdtc.org/debar059.htm