The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

Volume 15, No. 4 April 2007

Compliance Readiness – Law Firms

Developing And Implementing An Internal Compliance Program To Address Economic Sanctions Concerns – Part I

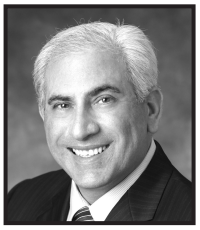
Edward L. Rubinoff, P.C. and Tamer A. Soliman

AKIN GUMP STRAUSS HAUER & FELD LLP

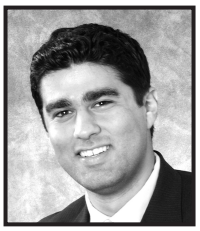
Editor's Note: Part II of this article will appear in the May issue of The Metropolitan Corporate Counsel. *Part II will set forth the elements of an effective internal compliance program and mention special issues that may need to be addressed by such a program. Parts I and II of this article are a condensation of a longer article by the same authors. An HTML version containing the full text of the longer article will be posted on our website at the time our April issue is being printed. The website version should be consulted for a more complete understanding of the issues as well as for additional cautions that should be considered.*

I. Introduction

The increasing integration of the world economy, combined with the increasing focus on security in the post-September 11th environment, provides U.S. businesses with a multitude of new business opportunities as well as higher risk of exposure. Companies pursuing business leads to the far reaches of the globe may return home to find themselves facing stiff fines and potential criminal prosecution for running afoul of U.S. economic sanctions laws and regulations. In addition, the dynamic political nature of U.S. sanctions law can mean that today's valued customer can become tomorrow's international outlaw.



Edward L. Rubinoff



Tamer A. Soliman

The need for an effective internal compliance program ("ICP") to avoid sanctions law violations has increased exponentially, driven by the increasing contact even small U.S. businesses have with foreign clients and the increasing focus on stemming the flow of financial resources to terrorist organizations in the post-September 11th environment. This article sets forth the general principles that should be observed when constructing an ICP, outlines the specific measures a company can adopt in its ICP, and describes special situations and transactions that should be encompassed by a sanctions ICP.

A. What Is An ICP and Why Should I Have One?

An ICP is a set of formalized policies and procedures developed to detect and prevent company violations of economic sanctions or export laws. The United States maintains a number of different regulatory schemes that restrict international trade in furtherance of various national security and foreign policy goals.

The departments of State, Commerce, and Energy manage export control programs designed to prevent the shipment of sensitive U.S. technology to certain foreign countries or end-users.

The Department of Treasury's Office of Foreign Assets Control ("OFAC") administers U.S. economic sanctions programs, which prohibit dealing, in whole or in part, with nations currently disfavored by the U.S. government.

OFAC currently administers comprehensive U.S. sanctions programs with respect to Cuba, Iran and Sudan as well as more limited sanctions against Burma, North Korea, the Palestinian Authority and Burma. In addition, OFAC administers controls against persons and entities designated as "fronts" for these countries, as well as persons "specially designated" on the basis of their affiliation with international terrorism (such as the Taliban and al-Qaeda); destabilization of the Balkans or the Middle East; weapons proliferation; and narcotics trafficking.

While export controls focus largely on the characteristics of the product itself and its country of origin, economic sanctions generally apply to the activities of "U.S. persons" wherever located, including company branch offices abroad. As a result, sanctions cover a far broader range of activity than export control regulations, including the provision of services, travel and financing, in addition to general prohibitions on the export of goods to the targeted countries. Many businesses that are not subject to export controls must deal with sanctions on a daily basis, most prominently in the banking and financial services industries. Therefore, the more comprehensive reach of sanctions requires U.S. businesses to look beyond their product lines and analyze virtually all commercial contact with targeted countries, regardless of the country

***Edward L. Rubinoff, P.C.** focuses on international trade policy and regulation and heads the firm's export control and economic sanctions practice. **Tamer A. Soliman,** Counsel, advises clients on U.S. law and policy affecting international trade and business.*

Please email the authors at erubinoff@akingump.com or tsoliman@akingump.com with questions about this article.

of origin of the goods, technology or services.

OFAC's regulations do not require a business to establish an ICP to prevent sanctions violations. However, failure to develop an ICP can lead to severe consequences. Depending on the sanctions regime, monetary penalties of up to $10,000,000 for each individual OFAC violation can be imposed, and company officials found guilty of violating OFAC regulations can face prison terms of up to 30 years. Moreover, even well-meaning companies can face substantial fines, since OFAC penalties can be imposed for inadvertent violations.

ICPs can prevent OFAC violations, and can mitigate the consequences in those instances where an OFAC violation occurs despite the use of an ICP. The Federal Sentencing Guidelines provide for a downward adjustment in sentencing for criminal violations where a company maintains an effective ICP. *See* United States Sentencing Commission, *Guidelines Manual,* §8B2 (2006). In addition, OFAC considers the presence of an ICP when imposing civil penalties. See *OFAC Economic Sanctions Enforcement Guidelines*, 68 Fed. Reg. 4422-4429.

An effective ICP therefore provides two significant benefits to a company: it prevents OFAC violations from occurring and mitigates penalties in those instances where an OFAC violation goes undetected.

II. General ICP Principles

OFAC recently published "Economic Sanctions Enforcement Procedures for Banking Institutions," which included a set of guidelines on effective compliance programs. 71 Fed. Reg. 1971, 1976 (January 12, 2006). Although those guidelines focused on financial institutions only, they highlight the importance of effective, tailored compliance programs for purposes of both prevention and mitigation. In any industry, building an effective, individualized ICP requires identification of the company's risk profile and incorporation of a few general core principles into the program.

A. Identification of ICP Issues—The Risk Profile

The first step in developing an OFAC ICP is identifying relevant business activities that can result in OFAC violations. OFAC violations can occur in the following circumstances:

• *Sales and Transactions for Goods or Services:* OFAC regulations generally prohibit the export or import of any goods or services from sanctioned countries. In addition, U.S. persons cannot enter into transactions with persons that OFAC has identified as being associated with a certain targeted country government or terrorist or drug activities. These individuals and business "fronts" are known as "Specially Designated Nationals" ("SDNs"), and OFAC provides a public listing of SDNs that is updated frequently.

• *Finance/Transactions:* OFAC regulations prohibit facilitation of financing of any transaction with a targeted country or SDN. In addition, U.S. financial institutions are required to freeze bank deposits and other assets in which targeted foreign governments or persons have an interest, and these blocked accounts may not be paid out, withdrawn, set off, transferred or dealt with in any manner without an OFAC license.

• *Travel:* OFAC prohibits transactions related to travel to some, but not all, targeted countries.

• *Vessels:* OFAC maintains a list of vessels that U.S. persons may not lease due to their connection to sanctioned countries or individuals.

• *Hiring:* U.S. companies or their branches may incur OFAC liability by hiring nationals of targeted countries or SDNs as employees or agents for their overseas operations.

In addition to identifying those business practices that are at-risk for OFAC violations, a company should also examine potential risk areas in its client base. Existing customers may pose OFAC violation risks due to their international dealings because OFAC regulations often prohibit even indirect facilitation of transactions with sanctioned countries or entities. New and little-known customers or clients may be SDNs or have dealings with SDNs or sanctioned countries. A thorough assessment of the company's customer base can also identify whether the company's business attracts high-risk customers.

A company should also identify products or services that it offers that may attract sanctioned countries. In addition, a company should examine its marketing practices for potential OFAC violation risks. Companies that market internationally or market to unknown customers can quickly find themselves engaged in solicitation or negotiations that are prohibited by various sanctions regimes. U.S. companies should also note that their overseas branches (but generally not subsidiaries) are considered "U.S. persons" subject to all OFAC prohibitions.

Finally, an assessment should be done of the risk-sensitivity of the company. A business should make an honest self-appraisal of how aggressive or conservative it is willing to be in pursuing business opportunities in sensitive markets. This assessment is driven by a number of factors, including the company's culture, the inherent nature of its business and its principal marketing areas.

B. Foundation For A Successful OFAC Compliance Program

Once the areas of potential OFAC liability have been established, a firm can begin to produce its OFAC ICP. When developing and implementing an ICP, a company should be mindful of four guiding principles.

Principle 1: Custom-Fit the ICP To Your Company.

The elements of an ICP must be designed to operate within the structure, culture and resources of the company in order to be effective. A small business' customer base may be limited enough to allow it to check the SDN manually and therefore make use of SDN detection software, commonly called "interdiction" software, unnecessary. A major multinational bank, on the other hand, as a practical matter should use interdiction software due to the volume of automated transactions it conducts each day.

Principle 2: Maintain a Flexible, Evolving ICP

A company must maintain a dynamic approach to its ICP and remain alert to OFAC changes in order for a program to retain its effectiveness. From the internal firm standpoint, a dynamic approach requires feedback, whether in the form of an audit or employee consultations, regarding where ICP procedures work, where they do not, and where alternate strategies may enhance efficacy and efficiency.

A company must also construct its ICP to remain alert to changes from OFAC. Sanctions regulations can change quickly, since they are driven primarily by political factors. A company can find itself in an increased realm of liability where new programs are implemented or existing programs are strengthened.

The listing of new SDNs is another area where OFAC changes can go largely unnoticed unless an ICP actively monitors OFAC information releases. The OFAC SDN list changes constantly as OFAC becomes aware of new front organizations and individuals. In addition, OFAC releases new SDN lists as conditions warrant, rather than updating SDN lists on a regular basis.

A dynamic and alert ICP also provides a decided competitive advantage in addition to preventing OFAC violations. Political winds blow in all directions, and recent years have seen sanctions policy lead to the loosening as well as tightening of sanctions regimes.

Principle 3: Keep the ICP Manageable

In order for an ICP to be effective, a firm must also ensure that it is manageable. In most contexts, this requires a centralized system of detailed review of transactions screened or "red flagged" by lower-level employees. Therefore, a manageable ICP often requires simplified procedures for many employees that forward questionable transactions to a centralized office for further review.

Principle 4: Ensure Upper Management Support for the ICP

The most customized, dynamic and manageable ICP will not succeed if the corporate hierarchy is not committed to ensuring OFAC compliance.