GENERAL OVERVIEW OF CONDUCTING INTERNATIONAL BUSINESS AT STORAGETEK

Introduction

As economic barriers between countries around the world have fallen, international trade and foreign direct investment have grown significantly. Companies conduct business internationally for a variety of reasons, whether defensively when faced with a threat to market share, or offensively to gain an advantage over competitors. Although expanding operations abroad in any form involves risk, the risk of not doing so may be even greater.

Entering the global marketplace requires U.S. companies to contend with complex issues under U.S. federal law, as well as with the laws of foreign jurisdictions. Conversely, foreign companies entering the U.S. must contend with the regulations of both their home jurisdiction and the U.S. These issues pose real challenges and involve real costs. However, forward planning and an awareness of what legal issues lie ahead can keep risk to a minimum. This material is presented as an introduction to identify some of the key issues we can expect to encounter as StorageTek expands its markets and operations. It is not a substitute for competent legal counsel experienced in the relevant areas of law.

General Principles

The following general principles will help guide you through the planning of international transactions.

Know your partner. Though important domestically, this is essential in the international context, where an untrustworthy partner, or a partner with different goals, can put StorageTek at tremendous risk of liability.

Identify all relevant legal regimes. This may not be as simple as it seems. Although the law of your "home jurisdiction," as well as the law of the "target jurisdiction" are both relevant, there may be multilateral or bilateral agreements (such as the European Community the General Agreement on Tariffs and Trade, the Bilateral Investment Treaty, the North American Free Trade Agreement, and the U.N. Convention on Contracts for the International Sale of Goods) or supranational organizations (such as the World Trade Organization, or the International Monetary Fund), that regulate the transaction. Civil law, as opposed to the common law system under which most U.S. lawyers are trained, may be applicable to the transaction. Lawyers trained in the common law usually encounter greater uncertainty in dealing with civil law jurisdictions because these jurisdictions lack the detailed interpretative guidance provided in common law jurisdictions. Furthermore, the transaction

may concern an industry with its own special regulations such as licensing requirements and approvals. The following industries usually are heavily regulated: Telecom, aviation, energy, banking, real estate, aerospace/ defense. Moreover, although legal principles in foreign jurisdictions appear at first blush to be similar to those in the U.S., critical differences do exist in the letter, application, and interpretation of even these principles.

Appreciate cultural differences. Understand the cultural norms of the jurisdictions implicated in the transaction. Cultural norms play a significant role in the style and procedure of negotiations. Awareness of cultural norms will indicate to your opposition that you are a sophisticated and experienced internationalist. It will also aid in managing outside counsel.

Remain politically aware. Keeping apprised of both the geo-political situation and the internal politics of the countries in which you plan to operate can keep you one step ahead of both obstacles and opportunities. Laws and agreements in many countries are interpreted in the context of, and are not free from the influence of, local politics.

Expect the unexpected. Doing business internationally often involves greater risk, and correspondingly greater potential rewards. The increased risk requires that StorageTek react quickly and effectively to changing situations.

Be cautious about trusting your instincts. Your instincts are based on your personal history, which probably has not encountered the issues with which you will be confronted in international transactions. For instance, a person who appears to be completely honest and trustworthy across the table in a negotiation may fully intend to be honest and trustworthy. However, cultural and social norms may dictate a different standard for honesty and trustworthiness than that which you expect.

Seek a measure of control, or at best, advantage. Attempt to control the primary incentive for your foreign partner through the initial negotiation. Seek to retain control of this incentive in the final agreement. Thus, if you are negotiating a cash deal, ensure that you control the cash until completion of all issues. Additionally, as foreign transactions always involve significant risk, allow an escape valve if the entire relationship disintegrates.

Because every transaction is different, this information is not meant to constitute an exhaustive list of issues that one might encounter, but rather a sampling of key issues that often arise in similar circumstances.

StorageTek Conducting Business Abroad

A. General Background Issues

In this section, we discuss several legal issues to keep in mind as StorageTek contemplates an international transaction. It is important to ensure that you are aware of these issues early on in the planning process to avoid surprise if and when they eventually arise.

1. Anti-Corruption and Anti-Terrorism

The U.S. government has stepped up enforcement of its anti-corruption and anti-terrorism measures. More and more, U.S. enforcement authorities are demanding that U.S. companies take affirmative steps to prevent the expanding range of activities that U.S. law proscribes. Penalties may be levied against the companies as well as the individual directors, officers, and employees who manage them. To the extent we use foreign sales agents or representatives we should be particularly sensitive to anticorruption measures, as entrenched cultural norms and business practices in many countries may run counter to these measures.

For these reasons, it is crucial for us to be aware of the changing regulatory environment, to know our partners, and to implement a comprehensive and effective compliance program to minimize the possibility of an infraction and to control the damage if and when an infraction should occur.

In this section, we briefly describe some of the major anti-corruption and anti-terrorism laws currently in force in the U.S., as well as appropriate company responses to both expanded regulation and government inquiries.

(a) The Foreign Corrupt Practices Act

One of the most important laws affecting U.S. companies expanding to overseas markets is the U.S. Foreign Corrupt Practices Act (the "FCPA"). The FCPA was enacted in 1977 in the wake of reports that many U.S. businesses were making large payments to foreign officials to secure business. It establishes two main principles: (1) a prohibition on bribery of foreign officials, political parties or candidates for public office for the purpose of obtaining or retaining business (the "anti-bribery provisions"), and (2) a mandate that companies required to file periodic reports with the Securities and Exchange Commission (the "SEC") establish and maintain accurate books and records and sufficient internal controls (the "accounting provisions").

Enforcement activities on the part of the U.S. Department of Justice and the SEC under the FCPA are increasing, and public comments by each of these agencies reflect their intent to expand enforcement activities.

Of primary importance, the FCPA imposes on a company an obligation to investigate certain types of suspicious activity. Once a company becomes aware of such "red flags," it must gather sufficient information to determine whether a violation has occurred. Violation of the FCPA can lead to severe civil and criminal penalties, including both monetary fines and imprisonment. It can also disqualify a party from receipt of government contracts as well as participation in both U.S. government-sponsored programs and procurements (such as those administered by the Overseas Private Investment Corporation) and programs administered by international financial institutions such as the International Finance Corporation and the European Bank for Reconstruction and Development. Finally, any organization convicted of violating the FCPA is likely to face a great deal of negative publicity.

(i) Anti-Bribery Provisions

With few narrow exceptions, the anti-bribery provisions of the FCPA generally prohibit any person subject to U.S. jurisdiction from corruptly making an offer or payment of anything of value to any

foreign official to obtain or retain business[1]. For U.S. companies, the critical elements of the anti-bribery provisions are usually the requirements that the offer or payment be made "corruptly" and to a "foreign official." Because the former requires a highly subjective determination, courts can infer intent from the facts and circumstances surrounding a transaction. Thus, in general, companies and their representatives should refrain from providing gifts to foreign officials. The FCPA defines foreign official quite broadly; it can include such persons as employees of the government or of a state-owned enterprise, a political party, or a candidate for political office. Corporate counsel should conduct due diligence to ensure that agents, representatives, and consultants of the company are not themselves foreign officials, as payments to such individuals to secure government contracts would constitute a violation of the FCPA.

(ii) Accounting Provisions

In addition to the anti-bribery provisions, the FCPA's accounting provisions require companies that make periodic filings with the SEC to "make and keep books and records, and accounts, which in reasonable detail, accurately and fairly reflect the transactions and dispositions" of assets[2]. The corresponding SEC rule provides that "[n]o person shall directly or indirectly falsify or cause to be falsified, any book, record or account subject to [this provision]."[3] The accounting provisions also generally require issuers to devise and maintain a system of internal accounting controls sufficient to prevent "unauthorized use or disposition of company assets and reasonable assurances that financial records and accounts are sufficiently reliable for purposes of external reporting."[4]

The requirement of internal accounting controls has three basic objectives: (1) books and records should reflect transactions in conformity with accepted methods of reporting economic events; (2) misrepresentation, concealment, falsification, circumvention, and other deliberate acts resulting in inaccurate financial books and records are unlawful; and (3) transactions should be properly reflected on the books and records in such a manner as to permit the preparation of financial statements in conformity with generally accepted accounting principles and other criteria applicable to such statements.[5] The SEC imposes a reasonableness standard rather than a materiality standard when enforcing this provision because the conduct that the section was intended to prevent, such as slush funds, off-the-book expenses, and unusual payments, may not rise to the level of financial statement materiality.

The FCPA requires an issuer holding more than 50 percent of the voting power of a subsidiary to cause the subsidiary to devise and maintain a system of internal controls. An issuer holding 50 percent or less of the voting power of a subsidiary must exercise good faith to use its influence, to the extent reasonable under the circumstances, to cause the subsidiary to devise and maintain such a system.

---

[1] 15 U.S.C. § 78dd-1(a).

[2] 15 U.S.C. § 78m(n)(2)(A).

[3] 17 C.F.R. § 40.13b2-1.

[4] *SEC v. World-Wide Coin Investments, Ltd.*, 567 F. Supp. 724, 750 (N.D. Ga. 1983).

[5] *Id.* at 748.

Understanding and complying with the provisions of the FCPA and similar legislation in other countries will be vital to ensure the success of international transactions in the years to come.

(iii) The Sarbanes-Oxley Act of 2002

In response to numerous recent corporate scandals, the U.S. Congress in 2002 passed the Sarbanes-Oxley Act ("Sarbanes-Oxley"). Because the accounting provisions of the FCPA are contained in U.S. securities laws, and because Sarbanes-Oxley mandates the implementation of new corporate safeguards for ensuring compliance with these securities laws, the requirements for FCPA compliance have been substantially modified by Sarbanes-Oxley. We therefore provide a brief overview of some of Sarbanes-Oxley's most relevant provisions.

a. Officer and Management Certifications

Sarbanes-Oxley requires certain officers of public companies to certify the accuracy of the company's financial reports and requires the management to provide an annual report on the company's internal controls. In this report, management must identify any "material weaknesses" in the company's internal controls. Quarterly reports must disclose any material change in the company's internal controls. In addition, public companies are required to adopt and maintain disclosure controls and procedures to ensure the timeliness and quality of both financial and non-financial disclosures.

Violation of the FCPA may trigger obligations under these sections of Sarbanes- Oxley. Often, the making of any inappropriate payment involves a violation of the accounting provisions of the FCPA because such payments are typically disguised by false entries in a company's books and records. Such false entries may be considered evidence of material weaknesses in a company's internal control over financial reporting or a failure of disclosure controls and procedures for the purposes of Sarbanes-Oxley.

b. Attorney Responsibilities

Sarbanes-Oxley imposes a responsibility on attorneys to report to the chief legal officer of the company evidence of a material violation of U.S. securities laws or breach of fiduciary duty or similar violations by the company or any agent thereof. This applies to both in-house and outside counsel. The chief legal officer is obligated to respond adequately to such evidence within a reasonable period of time. An adequate response could include appointing outside legal counsel to investigate and taking appropriate remedial measures. If an adequate response is not provided within a reasonable period of time, the reporting attorney must report to a higher authority, such as the company's audit committee or board of directors. The SEC asserts that this reporting requirement supercedes state ethics requirements, but this assertion is under attack by some members of the legal community.

c. Corporate Code of Ethics

Sarbanes-Oxley requires a public company to disclose in its annual report whether or not it has a code of ethics for its senior financial officers and its principal executive officer. Changes in or waivers (including implicit waivers) of such code must be reported to the SEC as well. Because corporate codes of ethics frequently prohibit bribery and related offenses, issues arising under the

FCPA will now have to be considered in light of a company's code of ethics, and the company must determine whether SEC reporting is required.

(b) Local Anti-Corruption Laws

For years, the U.S. was one of the only countries that prohibited bribery of foreign officials, creating a perceived disadvantage to U.S. companies. More and more, however, other countries are following suit and outlawing corrupt practices in international transactions. For example, as of 19 June 2003, 34 countries had ratified the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions of the Organisation for Economic Co-operation and Development, and 33 countries, mostly in Western Europe, had enacted full implementing legislation. The Convention contains bribery prohibitions similar to those found in the FCPA.

Because of the growth of anti-corruption laws around the world, many countries prohibit conduct that may be permissible under the FCPA. Not only do violations of local law fulfill the requirement of corrupt intent under the anti-bribery provisions of the FCPA, but they also carry their own costs, both in terms of legal penalties and negative publicity.

Experience has shown that once foreign officials are aware that a given company is willing to pay bribes, payment demands increase. Likewise, a company that lets it be known that it is unwilling to violate anti-corruption laws tends to encounter fewer such requests.

(c) Money Laundering

The U.S. Congress recently broadened the scope of U.S. money-laundering laws, and some courts have followed suit. Generally, U.S. money-laundering laws prohibit persons from engaging in transactions involving proceeds derived from criminal activity when such persons know that the proceeds are so derived and that their owner intends to disguise their nature. The elements of a money-laundering violation in the U.S. are listed below.

1. Transaction. This includes almost any disposition of anything of value. Although U.S. law extends only to transactions with a jurisdictional nexus to the U.S., courts have been quick to find such a nexus from the slightest contact with the U.S.

2. Criminal Proceeds. This requires the involvement of proceeds from specific crimes, including a wide variety of felonies such as FCPA violations, foreign tax evasion, and various forms of fraud, in addition to crimes such as drug trafficking.

3. Knowledge of Illegality. The defendant must know that the proceeds are the result of criminal activity. In addition to proof by direct evidence, knowledge can be inferred both from the collective knowledge of a company's employees or from willful blindness. Thus, failure by a company effectively to gather and evaluate available information, or failure to investigate red flags surrounding a transaction or a party, can suffice to prove this element.

4. Knowledge of Purpose. The defendant must know that the owner of the funds intends to disguise their nature, location, source, ownership, or control. One court has held that this element is obvious once knowledge of illegality is shown. Although it is too early to

know whether such a lax standard will prevail in the courts, knowledge may be inferred from facts and circumstances, especially by failure to investigate in light of red flags.

Some common red flags regarding money laundering are as follows:

- Unusual secrecy surrounding the transaction;
- Structuring the transaction to avoid attention;
- Depositing illegal profits in the bank account of a legitimate business;
- Highly irregular features of the transaction;
- Using third parties to conceal the real owners of funds; and
- A series of unusual financial moves culminating in the transaction.

The appearance of any of these or similar phenomena should prompt a thorough investigation to ensure the propriety of the transaction.

Thus, once again, it is essential to know your partner. This may require conducting sufficient due diligence to assure yourself that entering into a transaction with another party will not subject StorageTek to unknown liabilities. Additionally, any funds derived from unknown or questionable parties must be scrutinized. It is also important to include in relevant transaction documents representations and warranties and other provisions to protect StorageTek. In the case of a transaction that is convoluted for legitimate reasons, those reasons should be well documented. Finally, as always, it is crucial to understand and comply with all relevant local law.

(d) The USA PATRIOT Act

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (the "USAPA"), enacted in October 2001, broadly changed many existing U.S. laws. Many of these changes are relevant to companies participating in the international market. We briefly summarize two of the USAPA's most relevant effects.

The USAPA greatly broadened the definition of "financial institution" for the purposes of money laundering such that the definition now includes many entities not previously considered to be financial institutions. Additionally, all financial institutions must develop internal compliance policies, procedures, and controls, must designate a compliance officer, must establish an ongoing employee compliance training program, and must establish an independent audit function to test that program.

The USAPA added certain export control violations to the list of predicate crimes for the purpose of money laundering. Thus, the use of proceeds from such violations can form the basis of a money laundering violation.

2. Export Controls and Sanctions

Numerous U.S. laws, broadly referred to as "export controls," place limits on the entities with which U.S. companies may do business, as well as the goods in which they may trade. Specifically, this body of regulations prohibits U.S. companies, and in some cases their foreign subsidiaries and business partners, from engaging in, among others, the following activities:

1. Doing business with certain countries without a license (e.g., Cuba, Iran, Libya, Sudan);

2. Doing business with certain people and other entities (e.g., Specially Designated Nationals, Denied Parties, etc.);

3. Exporting certain types of goods without a license (e.g., the export – even to Canada of certain forms of ricin, a deadly toxin, requires a license);

4. Exporting or re-exporting certain types of goods to certain countries without a license (e.g., exporting high-tech computers to China is prohibited); and

5. Complying with, or agreeing to comply with, one country's prohibitions on sales or services (i.e., a boycott) to a country that is friendly to the U.S. (such as an Arab League country's boycott of sales to Israel).

In addition to a long list of controlled products, the government also regulates the transfer of technology and data. Under U.S. law, an export can occur entirely within the borders of the United States, or through electronic means of communication. For example, communicating technical data in a conversation with a foreign national – even if that foreign national is an employee of the company – could be a "deemed" export. As a result, a company working with controlled technology, technical data, or equipment must ensure that it does not permit the disclosure of such items to employees who are foreign nationals.

As most counsel to international corporations know, export control regulations are very complex and subject to frequent change due to the highly political nature of the national security interests involved. The Department of Commerce's Bureau of Export Controls, the Department of State's Office of Defense Trade Controls, and the Department of Treasury's Office of Foreign Assets Control are the main agencies in charge of these regulations. These agencies interpret very broadly the regulations that they enforce, and significant new enforcement activity has occurred in the last two years. New funding has been dedicated to the enforcement of export violations, and many U.S. companies have faced significant financial penalties as a result of inadvertent violations, even when they were voluntarily disclosed to the government.

3. Tax Considerations

Tax considerations are often central to a transaction. However, their complexity is multiplied in the cross-border context. Thus, it is crucial to obtain competent international tax advice right from the start. Below, we provide an introduction to some issues that might arise.

(a) Transfer Pricing

Transfer pricing is a means of allocating profits and transacting business with related entities based on the arm's length principal. There are specific guidelines promulgated by the governments worldwide as well as other international bodies (e.g., the OECD) that StorageTek must comply with. The Corporate Tax Department is responsible for compliance with these transfer pricing guidelines and rules on a worldwide basis.

An example of abusive transfer pricing that ignores the arm's length principle is as follows. One subsidiary of a company creates semi-finished products in a country with a very high profit tax, then sells the semi-finished products to another subsidiary located in a country with a lower profit tax, for completion of the product and export. The parent company sets the price at which the semi-finished product is sold to the second subsidiary very low, reducing taxable profits in the high-tax country and increasing taxable profits in the low-tax country. To avoid the perception that StorageTek is engaged in any such activities, the Corporate Tax Department needs to review and approve all inter-company transactions.

(b) Foreign Tax Credits

The U.S. permits U.S. companies to take credits for certain taxes paid in certain foreign jurisdictions. Many other jurisdictions have similar provisions regarding taxes paid elsewhere.

(c) Local Taxes

It is important to comply fully with all local tax laws in jurisdictions where StorageTek's operations may create tax liabilities. Furthermore, the tax laws of a jurisdiction might determine the nature of the entity your company establishes overseas. For instance, it may be more favorable to establish an overseas division of your company rather than a separate subsidiary, so as to avoid taxes on the separate entity of the subsidiary. On the other hand, many jurisdictions tax intra-corporate payments as if they were distributions to separate entities. Also, some jurisdictions may impose a level of taxation on sales, such as a Value-Added Tax, that must be accounted for in pricing determinations.

Some countries offer tax holidays to encourage investment. These tax holidays can be in the form of tax deferral, tax-free zones, foreign tax credits, etc. Tax holidays are often viewed suspiciously by the local populace, are often used by political opposition to attack incumbents, and can be repealed once investment has been made.

4. International IP Protection

Intellectual property ("IP") is an increasingly important aspect of international transactions. The fact that the protections afforded to IP in various jurisdictions differ widely increases the importance of ensuring its protection in those jurisdictions in which both your company and its customers and partners will operate. Furthermore, although some jurisdictions have legislated IP protective measures, cultural, political and economic factors sometimes dictate that these measures are not enforced. For instance, in Asia, although many jurisdictions provide for a system of IP protection, the imperative of obtaining cheap modern technology discourages enforcement of these measures.

Protection of IP rights could require registration in foreign jurisdictions (or in an international registry), creative drafting of licensing agreements, the inclusion of specific representations and warranties in agreements, or other steps.

5. Advertising

Many countries impose much greater restrictions on advertisers than the U.S. For example, some countries require that any performance claims be readily demonstrable, and some prohibit comparisons with competing products. Even where local law is more permissive, custom and public opinion may advise against the use of aggressive or comparative advertisements. Thus, once again, it is important to conduct a review of local law on this issue before embarking on an advertising campaign in a foreign jurisdiction.

6. Privacy

To the extent that we are doing business in Europe, we should be mindful of the stringent requirements placed on protection of information that is considered private by the European Union ("EU"), which has adopted various Directives relating to data protection. The most widely applicable of these Directives is Directive 95/46/EC of 24 October 1995, which relates to the protection of individuals in the "processing" of their personal data and the movement that data.

"Processing" includes many activities routinely performed by businesses in the employment context, including collection and/or storage of payroll records, performance evaluations, resumes, disciplinary actions, as well as the monitoring of employee e-mail or Internet access. In addition, the processing of sound and image data (such as photographs) in the employment context and the video surveillance of employees also fall within the scope of this legislation.

The Directive applies to the personal data of any "identifiable" person, including both private and public employees. Statistical reporting relying on aggregate employment data and/or the use of anonymous data does not constitute personal data. Further, the privacy of personal data extends to data subjects regardless of their nationality or residence.

The Directive requires businesses to register with government authorities prior to the processing of personal data. It also provides the employee with unfettered access to his or her data, to information about the recipients of the data, and permits the employee to block the transmission of any data. It requires that the employer keep the data secure both in storage and in transmission, and prohibits completely the processing of sensitive data such as that on ethnicity, race, religion or sexual preference. Finally, it prohibits the transfer of data to countries that do not afford employees an "adequate level of protection" of this data. As a result, transfers to the U.S. are allowed only if a company is able to take advantage of one of the Directive's Safe Harbors, which are available to those businesses that have developed significant technical and policy safeguards for the information.