Business and Litigation Update Spring 2011

PUBLISHED ON
January 1, 2011

TABLE OF CONTENTS

Expanding Your Business Through a Joint Venture: A Primer on Key Issues

By: Troy B. Rider

Due, in part, to the recent economic down turn, companies are increasingly investigating alternative routes to enhanced market share, supplementing strategic alliances and acquiring and strengthening other competitive advantages. One such route is the use of a joint venture. Legally, a joint venture is a commercial collaboration in which two or more unrelated parties pool, exchange, or integrate some of their resources with a view to a mutual gain, while at the same time remaining independent. Despite a rather simple definition, a well structured joint venture requires the participants to consider a number of complex issues.

The first topic to consider is the scope or the purpose of the joint venture. Specifically, the parties should determine what activities the joint venture will engage in, or, more importantly, what activities the joint venture will not engage in. Since most joint venture participants operate more than one line of business, having a well-defined purpose aids the parties in examining the potential and existing conflicts of interest between the joint venture and the parties' lines of business. In addition, a well-defined purpose also aids the parties in determining the scope of the parties non-competition and confidentiality obligations.

The purpose of a joint venture may also be shaped by certain laws. For instance, the United States Department of Justice has issued "Antitrust Guidelines for Collaborations Among Competitors." Similarly, the European Commission issued "Guidelines on Horizontal Competition Agreements." The Department of Justice guidelines summarize the law on competitive collaborations (which include joint ventures) and the government's approach to enforcement pertaining to joint ventures. In assessing the permissibility of an arrangement between competitors, the Department of Justice looks at the relevant market shares and market concentration in terms of whether the arrangement may create or increase market power. Assuming no per se illegal arrangements are involved, however, the Department of Justice does not challenge a competitor collaboration when the market shares of the collaboration and its participants collectively account for no more than twenty percent (20%) of each relevant market in which competition may be affected. Consequently, two large independent co-venturers that operate in the same market should be cautious of the Department of Justice's guidelines in forming and operating a joint venture.

Once the scope of the joint venture is established, the parties should consider the form of the joint venture. Essentially, a joint venture can take one of two forms, a co-ownership model or contractual. The co-ownership model is similar to the common law partnership where the assets, liabilities and obligations of the joint venture are split equally between the parties. Reality, however, dictates that the parties often contribute different levels and types of assets to the joint venture, therefore requiring a more concrete road map for defining the rights and obligations of each joint venturer. Consequently, the typical form of joint venture is the contractual form derived from a shareholders' agreement, bylaws, operating agreement or other governing document depending on the specific entity selected. Some of the common issues that should be resolved via the contract are (i) the specific assets contributed, including cash, inventory, labor, technical expertise and intellectual property, (ii) whether the joint venture requires financing and how such financing may be obtained, including the maximum amount of any permitted financing, (iii) the permitted or required use of capital calls among the parties and how such capital calls may be initiated, (iv) ownership rights of any property acquired or developed by the joint venture, (v) defaults by either joint venture, (vi) distribution of profits (or reinvestment in the business), (vii) management/governance of the joint venture, which is often dictated by the specific entity chosen (i.e., corporation, limited liability company, or partnership), and (viii) exit and termination rights.

At the outset, the parties are often reluctant to consider a default scenario or their respective exit and termination rights. The parties, however, cannot predict the future and achieving their respective strategic objectives may require that either of them leave the venture. For instance, the party's individual objectives may change, technological advances or development may not occur, or other co-venturers may change the management, objectives or ownership of the joint venture. Exit and termination rights are particularly critical where one co-venturer is clearly stronger than others. In that case, the weaker co-venturer will undoubtedly prefer to have exit rights clearly delineated in the agreement.

Regardless of the form of the joint venture selected, the parties should set forth their expectations in a letter of intent. All key provisions of the arrangement should be covered since it may be difficult to introduce a new or additional points once the letter of intent is signed. In addition, each party should consider conducting some level of due diligence on the other party. The parties should be comfortable with, for example, the organizational culture of the other co-venturer, especially if the joint venture involves domestic and foreign organizations.

The issues highlighted in this article are only a few of the important details in forming a well-structured joint venture. Each potential joint venture will require an analysis and determination of issues critical to the particular nature of that transaction, including potential tax ramifications for the parties involved. While a properly structured joint venture will not guarantee success, it will mitigate a number of future detrimental events that may hinder the joint venture's operation.

Back To Top

Fiduciary Duty in the New Millennium

The challenges to our economy brought by the corporate scandals of Enron, Worldcom and other large public companies, and more recently by the collapse of the housing and stock markets, have to striking developments in the law on fiduciary duty and, according to some commentators, the need for even more change. Before you can understand the implications of these changes, it is necessary to have a firm grasp of the traditional concept of

fiduciary duty.

Traditional Fiduciary Duty Principles

The traditional concept of fiduciary duty under Delaware and Pennsylvania corporate law can be summarized as consisting of two duties: the duty of loyalty and the duty of care. Generally, these duties seek to ensure that the corporation is managed for the benefit of the shareholders. The duty of loyalty requires directors and officers to act in good faith and in the best interests of the company, and not to use their positions to further their private interests. The duty of care requires directors and officers to fully inform themselves of all material information reasonably available before making decisions. A final principle to note is that majority shareholders are viewed as owing a fiduciary duty to deal fairly and not to exploit or oppress minority shareholders.

The Business Judgment Rule

Both the Pennsylvania and Delaware courts adhere to the "business judgment rule," which establishes a broad scope of authority and discretion for the board of directors. The rule establishes a presumption that, in making a business decision, the directors of a corporation have acted on an informed basis, in good faith, and in the honest belief that their decision is in the best interests of the company. However, the business judgment rule will not protect directors if they violate either their duty of care or their duty of loyalty. Furthermore, a court will take a more direct and active role in overseeing the decisions made by directors in situations where either of the following occurred (1) the approval of a transaction resulting in a sale of control or break-up of a company; and (2) the adoption of defensive measures in response to a threat to control the corporation. The first situation results in what are known as "*Revlon* duties" and the second in "*Unocal* duties," after the Delaware cases by those names decided in the mid 1980's. Where these duties arise, the burden is on directors to prove, without the presumption of the business judgment rule, that the board exercised its fiduciary duties of loyalty, good faith, and care in its decision-making process.

Delaware *Caremark* Claims

The development of *Revlon* and *Unocal* duties, though significant, does not represent a major departure from the traditional concept of fiduciary duty because it does not deviate from the fundamental premise that state law fiduciary claims must be based on corporate violations of state civil law. More recent case law, by contrast, indicates a growing acceptance of the theory that such claims may be based on violations of *federal criminal law*. This fact is demonstrated by the proliferation of so-called "*Caremark* claims," i.e., derivative cases based on (1) liability that "follow[s] from a board decision that results in a loss because that decision was ill advised or "'negligent'"; or (2) liability "from an unconsidered failure of the board to act in circumstances in which due attention would, arguably, have prevented the loss." The second type of liability is problematic because it may arise out of a director's failure to ensure that a corporation's information and reporting system is adequate.

A 2006 Delaware Supreme Court decision, *Stone v. Ritter,* illustrates this problem. In that case, a plaintiff accused the directors of a bank of breaching their fiduciary duties by failing to institute sufficient internal controls to guard against violations of the Bank Secrecy Act and anti-money laundering regulations. In practical terms, federal liability in Stone was caused by lower-level employees allowing customers to use the bank to run a Ponzi scheme. Even though the plaintiff did not prevail, this case is noteworthy in that the plaintiffs alleged the directors should be held liable for the fact that the company was indicted for violations of

the federal Bank Secrecy Act. The claim in *Stone* is a typical example of a federalized *Caremark* claim, which is based solely on the announcement of a federal investigation or indictment, without substantiation of the alleged illegal acts.

Honest Services Fraud Cases

Another development in the law of fiduciary duty that is a subset of the federalized *Caremark* claim is the enforcement of fiduciary duties through criminal prosecution of honest services fraud under 18 U.S.C. 1346. Section 1346 is a controversial statute that makes it a felony to engage in a scheme "to deprive another of the intangible right of honest services." Although Section 1346 does not reference state law fiduciary duties, courts have usually restricted honest services fraud to cases where such a duty existed. However, in 2008 , the Seventh Circuit in *United States v. Sorich,* asserted that other sources besides state law can create a fiduciary obligation between a public official and the public or between an employee and employer in honest services cases. The court in *Sorich* cited federal cases where employee handbooks or power of attorney agreements were sources of fiduciary duties. Because of the growing number of cases brought under this statute against directors, officers, employees and public officials, and the numerous interpretive questions that divided the federal appellate courts, the Supreme Court granted certiorari in three cases involving honest services law and consolidated them into one opinion in *United States v. Skilling.*

In *Skilling*, the former president of Enron Corporation had been convicted in the United States District Court for the Southern District of Texas of conspiracy, securities fraud, making false representations to auditors, and insider trading. The Supreme Court decision held that Skilling did not commit honest services fraud by allegedly conspiring to defraud Enron's shareholders by misrepresenting the company's fiscal health and thereby artificially inflating its stock price, where there was no allegation that Skilling solicited or accepted bribes or kickbacks from a third party in exchange for making those misrepresentations. The Court refused to accept the government's argument that a simple financial conflict of interest was sufficient to create liability under Section 1346. The Supreme Court's ruling sounds deceptively simple, as it will lead to much litigation over exactly what constitutes kickbacks and bribery.

Fiduciary Duties for Minority Shareholders

In addition to the growing number of cases that criminalize breaches of fiduciary duties by directors, officers, public officials and employees, there is another development in the case law of multiple jurisdictions concerning duties of minority shareholders. Traditionally, courts tend to find that "controlling" shareholders are subject to the duty of loyalty, while "non-controlling" shareholders may vote however they choose without any argument that their motives are for personal gain. The rise of institutional investors (such as pension and mutual funds) that aggregate the savings of millions of individuals into large portfolios that buy stock in public companies demonstrates that minority shareholders can in fact be influential. Fidelity and Vanguard, for example, repeatedly mount public relations campaigns, initiate litigation, and launch proxy battles to pressure corporate officers and directors into following their preferred business strategy. In addition, the 1992 amendments to federal proxy regulations, by removing barriers to public statements and other communications, have made it easier for institutional investors and hedge funds to coordinate with each other and combine their holdings into a larger voting block. Many hedge funds typically take large positions in two or three companies, and then demand that those companies pay special dividends, sell assets, and take other actions that maximize "shareholder value."

In spite of the conflicts of interest that fuel the influence of institutional investors and hedge funds over corporate policy, the trend towards greater power for minority shareholders shows every sign of continuing with the possible adoption of "proxy access" rule by the Securities Exchange Commission and the New York Stock Exchange's proposal to eliminate "broker voting". These changes are in response, in part, to the corporate scandals that are brought before the court as *Caremark* claims or as honest services violations under Section 1341. Commentators suggest that imposition by the courts of a fiduciary duty upon all shareholders will balance the need to give shareholders the ability to stop management fraud against the concern that certain shareholders will use this power to benefit themselves.

Back To Top

Data Breaches: A Matter of When, Not If

By: Donald R. Geiter, CIPP/US

Nearly every company routinely handles electronic data containing personally identifiable information. This data can include information about its customers, employees, or business partners. Whether a company is actually collecting and sharing the data itself or merely handling and storing data collected by others, there is the potential that this data may fall into the hands of unauthorized third parties -- a data breach.

Is your company aware of data breach notification requirements and prepared to appropriately respond to a data breach?

In the last five years alone, hundreds of substantial data breaches have resulted in the compromise of hundreds of millions of data records containing personally identifiable information. Some of these breaches were a result of human error, such as the misplacement of an employee laptop or smart phone. Other breaches were a result of illegal or malicious activities. The cost to a company for a single data breach can be staggering. For example, one of the largest data breaches in the United States will cost TJX Companies up to $500 million. In TJX's case, third parties accessed and stole customer credit and debit card data and used it to make unauthorized transactions. TJX settled several class action lawsuits filed by customers, as well as lawsuits filed by financial institutions that had to reissue millions of credit and debit cards. In addition to damage awards in private lawsuits, such as the case with TJX, companies can also be held responsible to pay hefty government-imposed sanctions. Also, a company cannot ignore the impact a data breach can have on its reputation and customer confidence and trust.

Having a proactive system of data security policies and procedures in place to avoid data breaches is paramount to a company. A system of policies and procedures will likely reduce the occurrences of data breaches and may serve to mitigate some of the costs of a data breach. However, no system of policies and procedures is perfect. Therefore, for most companies the next important question is "what will we do when a data breach occurs?"

In developing its data security policies and procedures, a company must be aware of the myriad of laws relating to the protection and sharing of data containing personally identifiable information. These laws include federal laws, such as the Federal Trade Commission Act, Gramm-Leach-Bliley Act, the Fair and Accurate Credit Transactions Act, and the Health Insurance Portability and Accountability Act. State laws include, but are not limited to, consumer protection laws, safeguard laws, social security number protection laws, disposal requirements (all of which will be discussed in future articles). Companies that collect personally identifiable information must also be aware of specific state data

breach notification laws that apply when a data breach occurs.

The relevant data breach notification law in Pennsylvania is the Breach of Personal Information Notification Act. This Act took effect on June 20, 2006, and applies to all types of companies, including for-profit and non-profit businesses, governmental agencies and financial institutions. The Act serves to protect data containing personally identifiable information that includes a resident's first name or first initial and last name in combination with some other data element that is not encrypted or redacted. These other data elements include a social security number, a drivers license number, a financial account number or a credit or debit card number with a security code or password. The Act describes a breach broadly to include an "unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personally identifiable information." The Act requires that upon discovery of a breach, or following the reasonable belief that a breach may have occurred, the company must provide notice without "unreasonable delay" to the resident whose personally identifiable information may have been compromised. The form of notice can vary -- it can be written, telephonic or via e-mail (subject to certain requirements). A company can employ a substitute notice method if the number of notices exceeds 100,000 or the number of residents affected exceeds 175,000. In addition to notifying the affected resident, if notification is provided to more than 1,000 residents at one time, the company must also notify all major reporting agencies. A violation of the Act constitutes a violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Act, which could result in treble damages and costs to the violating company.

Most states and the District of Columbia have enacted their own laws relating to data breach notifications. While there are several common notification obligations across the various sets of state law, many states have enacted unique provisions that require a specific response if a resident of that state was affected by the breach. Consequently, if a company handles personal identifiable information of residents from various states, upon a data breach, the company must follow the breach notification laws of each of the relevant states. In addition to requiring notice to affected persons, some states also require notice of the breach be made to certain state agencies and law enforcement authorities. Furthermore, business regulated by certain governmental authorities may have additional data breach notification requirements.

Each data breach is different and a company's response must be tailored to the unique circumstances presented by each data breach. It makes most sense for companies to become aware of data breach notification requirements in connection with the development of its comprehensive data security policy and procedures. Contact us for more information on responding to a data breach, or general questions relating to data security policies and procedures.

Back To Top