Hunton & Williams
Client Alert

January 2009

Contacts

Peter Brudenall
30 St Mary Axe
London EC3A 8EP
United Kingdom
+44 (0)20 7220 5725
pbrudenall@hunton.com

James A. Harvey
Bank of America Plaza, Suite 4100
600 Peachtree Street, NE
Atlanta, GA 30308-2216
(404) 888-4160
jim.harvey@hunton.com

Randall S. Parks
Riverfront Plaza, East Tower
951 East Byrd Street
Richmond, VA 23219-4074
(804) 788-7375
rparks@hunton.com

What to Do with Your Satyam Agreement

On January 7, world markets were stunned by the announcement by Ramalinga Raju, the chairman of India's fourth-largest outsourcing vendor, Satyam Computer Services (NYSE: SAY), that the company's accounting records had been riddled with fraudulent numbers for years. In a letter written to Satyam's board of directors and distributed by the Bombay Stock Exchange, Raju stated that some 50.4 billion rupees, or $1.04 billion, most of the cash and bank balances that Satyam had listed as assets in its second-quarter earnings report, were nonexistent. Raju further admitted that Satyam had significantly inflated its revenues, operating margin and accrued interest, and significantly understated its liabilities. The chairman stated that neither the board nor other Satyam executives had knowledge of the fraud.

Satyam obviously will be challenged in the coming months. While Satyam's president, Ram Mynampati, has attempted to rally the company and some partners (such as Oracle) have expressed support, the company's future is unclear and likely will remain so for some time. In light of that uncertainty, we recommend that our clients and friends who may have, or be considering entering into, contracts with Satyam take the following immediate action:

- evaluate your exposure to Satyam;
- consider future scenarios;
- check your options; and
- develop a response plan.

Evaluate Your Exposure

As a threshold matter, your response to Satyam's problems will depend on:

- the scope and status of your agreements with them;
- the importance to your business of the services they perform; and
- the sensitivity of those services to potential disruption.

Obviously, your exposure is much different under a BPO arrangement with a seven-year term than it is under an application development agreement terminable on 30 days' notice. However, short-term contracts with relatively small value may involve handling of highly sensitive customer data or relationships or support of mission-critical applications, the loss or disruption of which would cause harm disproportionate to the value of the contract. It is also not uncommon for relatively low-value agreements to expand through additional work orders — none of which may have passed through the legal department. Also, Raju's letter to his board claimed that the accounting misstatements were confined to the holding company and that the books of the operating subsidiaries were correct. If the corporate firewalls hold, understanding whether your agreement is with the Indian parent or a US or other subsidiary may be important. Reviewing the complete contract file and enlisting technical and business resources to evaluate practical exposures will be critical.

Consider Future Scenarios

The resolution of Satyam's crisis may take any number of paths. "Business as usual" seems highly unlikely. Existing customers may look to end their relationship with Satyam over the next three to six months. Important Satyam employees may also move on to other vendors, taking away significant client relationships and intellectual capital. The company will also be under legal stress in the US, with several class-action lawsuits reportedly already on file.

Some sort of strategic transaction may be the eventual outcome — a significant investment by a white knight or a sale as a whole or in parts to financial investors or competitors. On the other hand, an insolvency proceeding could be instituted under Indian or other applicable laws. Indian insolvency proceedings are unlike US reorganizations under Chapter 11 and may offer fewer prospects for continuing operations. In the worst case, the enterprise could simply cease operations and be completely liquidated. Since there is no certainty which path the company will take, customers should adopt a risk-adjusted response that reflects their practical exposure to one or more of the possible downsides of a Satyam relationship and the services it provides. If you are significantly exposed and a loss of services would cause significant disruption, caution would dictate immediate action to secure key resources and implement back-up plans.

Check Your Options

Engage Your Account Team. Your Satyam account team will be the best source of information on the state of affairs at Satyam and Satyam's own risk-management efforts and remediation options. Engaging team leaders and, if necessary, Satyam management, in a frank discussion of your concerns and their ability to respond to those concerns will be an important first step.

Review Contract Rights. Well-constructed agreements should offer a number of direct and indirect opportunities to manage risks. While commentary in situations like this often focuses on termination rights, many customers may be more focused on achieving additional contractual protections for a continuing relationship. Termination rights — whether arising from the current situation or past missteps — may provide the negotiating leverage to achieve that end. Your contract rights may include:

- Financial covenants or a "material adverse change" clause permitting early termination in the circumstances now facing Satyam, without payment of a fee.
- Termination for convenience rights, perhaps upon payment of a fee. While Satyam might be economically indifferent to a termination for convenience accompanied by a termination charge, you might find them willing to make concessions simply to retain the customer relationship and avoid the additional negative press associated with an early termination.
- Service level commitments. Where a vendor is unstable, objective service levels serve as early warning signs of performance problems. Service-level defaults may also create termination rights.
- The ability to create new service levels. Consider adding additional service levels to address key uncovered areas. Because these provisions often require substantial advance notice, quick action to start the process may pay dividends as events unfold.
- Account team continuity requirements and workforce turnover limitations. Contractual commitments to maintain account team members in place and limit workforce turnover are important to maintaining the team's knowledge base and the quality of service. Default on these commitments would be a key sign of trouble.
- Transfer of software ownership rights upon development, rather than delivery or payment, especially when accompanied by provisions requiring periodic (daily) delivery of code and audit rights. These provisions reduce dependence on continuing vendor viability and limit the risk that key software work-in-process will be lost or tied up in legal proceedings. Be sure that applicable intellectual property rights assignments are in place, especially in India, where proper assignments are critical to perfecting ownership rights.
- Data retransfer provisions requiring delivery of customer data on demand. Periodic data delivery requirements (perhaps effected through data mirroring to customer sites or other backup procedures) manage the same risks to data described above for software work-in-process.
- Provisions requiring access and audit rights.
- Rights on exit. It is common for outsourcing agreements to include obligations on the vendor to provide and maintain a plan for dealing with the termination of the contract, and the transition from one vendor to another. You will need to ensure that any such plan is up to date and review whether it adequately caters to a requirement to transition quickly to a replacement service provider.
- Provisions relating to step-in. Most outsourcing agreements also allow for the customer, or a third party on behalf of the customer, to "step

in" and take over the services for a period of time, when there has or may be a disruption to the services. Such rights could be triggered if the service begins to deteriorate.

If your contract doesn't include some or all of these provisions, now is the time to seek protective amendments. A review of contract compliance may also reveal additional options under existing rights — or provide comfort as to Satyam's ability to perform.

Review Insurance Coverages

Your insurance policies and those required to be maintained by Satyam may offer coverage for potential losses. Take steps to assure continuity of coverage and focus on delivering appropriate notices to carriers.

Monitor Performance

Since Satyam's situation may change rapidly and often, real-time performance monitoring will be critical. Evaluate existing management and reporting mechanisms to be sure that they cover all key operational measures and that they are delivered with sufficient frequency. While monitoring service levels will be important, pressures on Satyam to cut costs may make verifying the delivery of all services (whether or not covered by service levels) more important.

Consider Self-Protection in the Worst Case

In the worst case, contractual protections that assume rational actors with long-term business strategies may prove ineffective. Consider positioning yourself to avoid the worst consequences in a meltdown by:

- securing data;
- securing developed code and work-in-process;
- collecting any credits now due, including a fresh inventory of existing defaults and overall performance levels of Satyam under the agreement;
- managing payment streams to your best advantage; and
- developing a plan for complete substitution of services, which might include a backup contract with an alternative vendor (e.g., adding one or more additional development services vendor to create a "stable" of available providers).

Conclusion

While this week's revelations raise questions about corporate governance at Satyam, they do not suggest that any other outsourcing vendor, whether in India or anywhere else, has similar problems. The bad accounting practices of one company should not taint the entire industry. Satyam may very well survive this episode, though perhaps in an altered form. In any case, the current spectacle ought to remind us all of the risks inherent in any significant long-term relationship and the importance of constructing protections not only against ordinary risks, but also against the lightning bolts that strike less often, but with devastating consequences.

We would like to thank Sajai Singh, partner with J. Sagar Associates, a well-known law firm in India, for his kind review and helpful insights in this article.

Hunton & Williams has organized a cross-disciplinary team of lawyers to respond to the Satyam situation, including leading outsourcing, data security and insolvency practitioners, as well as local counsel in India. Our Global Technology, Outsourcing and Privacy practices, in concert with The Center for Information Policy Leadership, provide players in this dynamic market with an unparalleled combination of resources to address today's sourcing challenges. Our innovative multi-pronged approach offers a comprehensive solution for global transactions. Our Global Technology and Outsourcing practice was ranked the #1 Outsourcing and Offshoring Legal Advisor in Brown & Wilson's *2008 Black Book of Outsourcing*. Our Privacy and Information Management practice is a leader in the field and was named the top firm for privacy by *Computerworld Magazine* for the third year in a row in 2008.

About Hunton & Williams

Hunton & Williams LLP provides legal services to corporations, financial institutions, governments and individuals, as well as to a broad array of other entities. Since our establishment more than a century ago, Hunton & Williams has grown to more than 1,000 attorneys serving clients in 100 countries from 19 offices around the world. While our practice has a strong industry focus on energy, financial services and life sciences, the depth and breadth of our experience extends to more than 100 separate practice areas, including bankruptcy and creditors rights, commercial litigation, corporate transactions and securities law, intellectual property, international and government relations, regulatory law, products liability, and privacy and information management.