LJN LAW JOURNAL NEWSLETTERS

Business Crimes Bulletin ®

An incisivemedia publication

Volume 16, Number 3 • November 2008

FCPA Due Diligence and Data Privacy Laws

How to Reconcile the Irreconcilable

By Jacqueline C. Wolff and Daniel P. Cooper

As Russia, China, India and a host of other countries open their doors to U.S. investors, the number of companies and individuals who need to think about the risk of prosecution under the Foreign Corrupt Practices Act of 1997 (FCPA) has increased tremendously. No longer is it just the big multi-nationals who need to consider FCPA compliance risks; private equity firms, individual investors, and small businesses looking to get a piece of the international pie need to understand the risks of potential criminal exposure before they invest overseas. That means understanding the requisites of due diligence.

This year the Department of Justice (DOJ) issued two important advisory opinions describing what due diligence a potential investor and an acquiring party had performed in order to obtain a "no enforcement" opinion from the DOJ. In this article we examine the inherent conflict between what the DOJ expects and the prohibitions placed on such due diligence by the privacy laws of other countries. We also suggest ways to deal with this seemingly insurmountable conflict.

Jacqueline C. Wolff (jwolff@cov.com), a member of this newsletter's Board of Editors, is a former federal prosecutor and of counsel to Covington & Burling LLP in New York City. **Daniel P. Cooper** is a member of the firm resident in its London office.

DOJ Opinion Releases

Under the FCPA, the DOJ must, when asked in writing, provide companies with advisory opinions stating whether a proposed transaction is in violation of current FCPA enforcement policy. The requesting company must disclose to the DOJ all the details of the proposed transaction. The DOJ has 30 days to respond. Although these opinions cannot be used as precedent by anyone other than the requesting company, they provide a window into how the DOJ exercises its prosecutorial discretion in FCPA cases.

In DOJ Opinion Procedure Release 08-01, issued Jan. 15, 2008 and posted at www.usdoj.gov/criminal/fraud/fcpa/opinion/2008, a U.S. investor sought to invest in a foreign private entity that was to be created by privatizing a partially state-owned company (the "Target"). The U.S. investor had been negotiating with the foreign individual who controlled both the private minority interest in the Target and the private entity that had been awarded the foreign government entity's shares in the Target during the privatization bidding process. The foreign individual had also been acting, without pay, as the Target's General Manager. His role in the Target made him a "foreign official" under the FCPA and thus raised the question of whether DOJ would deem the premium he would receive upon the proposed U.S. purchase of his shares in the Target to be an illegal payment under the FCPA even though he would lose his "official" status as soon as the proposed transaction was consummated.

In the Release, the DOJ set forth several factors underlying its opinion that the proposed transaction would not prompt enforcement action. One factor was that the U.S. investor had determined "after reasonable inquiry" that no officer, director employee, consultant, representative or agent of the foreign entity from which it sought to purchase shares in the Target, and no "close relative" of the individual with whom it had been negotiating, was a foreign official. Such a representation necessarily required the investor to gather personal information from people affiliated with the private entity, including questions about their family members' affiliations with government entities and political parties.

A similar expectation that personal questions will be asked and answered is shown in Opinion Procedure Release 08-02. Halliburton was seeking DOJ reassurances for a proposed acquisition of a UK company where local law made it difficult to determine if the target company had a history of FCPA issues. In addition, a pre-acquisition confidentiality agreement prevented Halliburton from reporting any such issues before the deal closed. The DOJ's opinion said it would not prosecute Halliburton for any past FCPA violations by the target company if, after the acquisition, Halliburton conducted a thorough internal investigation and reported any past violations to the DOJ on a 90-, 120- and 180-day schedule, starting with high-risk areas. This naturally would require Halliburton to investigate overseas employees, consultants, agents and third parties with which the target did business regarding their own and their close family's "foreign official" status as well as their past criminal conduct.

The take-away from these Releases is that in order for a potential investor or acquirer to avoid prosecution for il-

legal payments under the FCPA, its due diligence must include getting answers to "personal" questions regarding family members and their affiliations with government entities and political parties and whether they engaged in criminal conduct in the past. They must also be prepared to provide those answers to a U.S. criminal enforcement agency. Yet, under European Union (EU) data privacy laws and similar laws in other countries outside the EU, asking such personal questions and supplying the answers to the U.S. authorities is not only inappropriate but may be criminal.

Data Privacy Laws

More than 80 countries, including the 27 Member States of the European Union, Japan, Australia, Switzerland, Argentina, Canada and Russia, have implemented data privacy laws regulating the collection and transfer of personal information. Draft legislation is pending in Mexico and China. The United States is quickly becoming one of the few major industrial nations without such laws, opting to enact sector-specific privacy laws instead of the comprehensive data privacy laws found elsewhere.

Most data privacy laws require the collection of any personal data to be justified on one of a limited number of so-called "legitimate" grounds. Collecting information to comply with U.S. laws is not one of them. In 2005, for instance, EU data privacy regulators specifically moved to prevent U.S. companies from collecting and transferring personal data to the United States through their internal whistleblower hotlines based on the Sarbanes-Oxley Act (SOX). Where the data qualify as "special" or "sensitive," which typically includes information relating to a person's association with a political party or commission of a criminal offense, even greater restrictions apply. This is just the kind of information that routinely is collected in FCPA due diligence.

Even where one can meet one of the permissible grounds for collection, data privacy laws place significant restrictions on its transfer outside the home jurisdiction. EU rules, for instance, prohibit the transfer of personal data to any non-EU jurisdiction that does not apply "adequate" protections to personal data. To date, EU authorities have not deemed U.S. law to provide adequate protections. So U.S. companies seeking to transfer data to the United States under the FCPA must provide adequate protections in some other way.

Foreign data privacy rules also require companies to ensure that their collection and processing of data is "proportionate" and generally takes place with the knowledge of the relevant individual. To conduct comprehensive FCPA due diligence, U.S. companies often need to deploy abroad detailed questionnaires and other investigative tools whose scope can offend the proportionality principles of foreign laws. Information gathered about individuals who often are unaware that personal data about them are being collected and disclosed to U.S. authorities, such as "close relatives" and family members of persons owning or managing an acquisition target, would generally not be deemed proportionate.

If found to have violated these foreign data privacy laws, companies may be subject to criminal or administrative fines or civil liability for damage or distress suffered by the relevant individuals. Regulators in the EU, in particular, appear to be applying their data protection laws more aggressively in recent months, especially where international transfers of personal data are involved. In Spain, for example, the national data privacy regulator has fined companies more than one million euros (nearly $1.4 million) for breaching Spanish law. Fines in the six-figure range have been reported elsewhere. Telefonica and Telefonica Data were both separately fined over 500,000 euros each for failing to adhere to Spanish data protection laws. The French authority CNIL imposed a fine in May 2007 on Tyco Healthcare of 30,000 euros for non-transparency and lack of compliance with data protection laws. In April 2008, Service Innovation Groupe France (SIG) was fined 40,000 euros.

Reconciling the Irreconcilable

What can potential investors and acquirers do? One avenue is to determine whether the conduct also violates local anti-corruption laws. If so, the due-diligence inquiry can be focused on those laws and meet one of the grounds that justify data collection in most jurisdictions. Second, companies can carefully restrict the scope of their due diligence to determining whether there has been an actual FCPA breach, thereby avoiding some of the more personal questions often asked at the peril of stopping a transaction in its infancy. Third, companies can incorporate data privacy notices or statements into their FCPA questionnaires and related forms, or possibly even seek the responder's express consent. Such privacy statements would say that the personal data provided may be transferred to U.S. enforcement agencies and reviewed for FCPA compliance. Companies also may put the onus on the target company to ensure that people whose data are being collected are provided with a privacy notice explaining why their data may be transferred to the United States.

Other possible compliance mechanisms include anonymizing and aggregating information to bring it outside the reach of data privacy laws, keeping and reviewing completed due-diligence questionnaires in the local jurisdiction, and putting in place measures like transfer contracts to protect information that is transferred to the United States. A company can also consider enrolling in the Commerce Department's Safe Harbor described at http://www.export.gov/safeHarbor. Taken together, these and other measures, although providing no guarantee, can help reduce the risk of violating foreign data privacy laws. EU data privacy regulators, for one, are now focused on the issue, so there may be further developments in the months ahead.