

COMPLEX LITIGATION & *E - Discovery*

Foreign Corrupt Practices Act Makes E-Discovery Readiness Planning Critical

Reduce risk with advanced
planning strategies

By Paul Brabant

Business continues to expand across international borders, and with it so does the scope of government investigations, litigation and corporate due diligence reviews. By now, most of us are well aware of electronic discovery, which continues to expand around the globe, and requires attorneys to be knowledgeable about how to identify, preserve, collect and possibly move information from foreign entities while managing risks and reduced budgets.

For global businesses with a footprint in the U.S., the Foreign Corrupt Practices Act ("FCPA") adds to the stakes. The FCPA, enacted in 1977, focuses on two primary issues: bribery of foreign officials and the recordkeeping associated

Brabant is senior vice president, eDiscovery, at Epiq Systems in Washington, D.C.

with such payments. The FCPA applies to issuers of securities traded on a U.S. exchange, and is jointly enforced by the U.S. Department of Justice (DOJ) and the U.S. Securities Exchange Commission (SEC). Violations of its provisions can result in significant fines for U.S. corporations, as well as prison time for individuals. In the last few years, the DOJ and SEC have broadcast a clear message to corporations by escalating the rate of enforcement, and publicly emphasizing that enforcement will no longer affect just the corporate entity, but will directly implicate corporate executives.

Two recent cases that involve companies with a New Jersey presence, Alcatel-Lucent SA and Daimler AG, underscore the risk of severe financial and criminal liability, the importance of compliance programs, and the ability to conduct investigations based on corporate data that is mostly maintained in electronic form.

In mid-February, the media reported that Alcatel-Lucent agreed to pay \$137.4 million and change internal procedures to avoid U.S. prosecution for alleged violations of the FCPA involving bribes paid in Costa Rica, Taiwan and Kenya, accord-

ing to a company regulatory filing. In a statement to *BusinessWeek*, the company said, "Alcatel-Lucent's new management has implemented vigorous compliance and training programs designed to prevent similar situations from happening in the future."

In April, Daimler AG and three of its subsidiaries agreed to a \$185 million global settlement to resolve allegations the companies paid tens of millions of dollars in bribes to foreign officials for a decade, according to news reports. Justice Department prosecutors said in March that Daimler "engaged in a long-standing practice" of paying bribes to foreign officials through corporate ledger accounts, offshore bank accounts and deceptive pricing arrangements, among other mechanisms, in violation of the Foreign Corrupt Practices Act.

The Link Between FCPA and Electronic Data

If a corporation has not yet dealt with any type of e-discovery matter, and has not felt the need to implement protocols and tracking mechanisms for electronic

data, an FCPA investigation will require that it abruptly take control of the situation. That exercise will come with a steep and costly learning curve, as FCPA investigations typically combine several challenging factors in addition to the demands of managing a routine electronic discovery response.

Initially, the primary focus must be to define a strategy to effectively investigate the allegations. Once past this hurdle, gathering necessary evidence could be even more time consuming and disorienting. Given the nature of FCPA violations, they involve global firms operating in multiple countries. Add several foreign languages, and legal jurisdictions with varying data protection laws, and you have a situation that could prove extremely disruptive.

The Value of a Compliance and Investigation Plan

A Compliance and Investigation Plan (“CIP”) is an important element of a successful response to a government inquiry. To date, the companies that have invested the time to create and implement such a plan are a minority. Corporations without such a plan face the risk of a protracted fire drill if they find themselves the unfortunate target of government investigation, particularly in connection with the FCPA.

As with any effort to prepare for litigation or regulatory compliance, the first step is to examine how information moves through the organization, and to determine how to identify the materials relevant to a particular issue. Practical experience tells us this is easier said than done, and always seems to cost considerably more than whatever anyone in legal or IT could predict. Once this identification process is under way, the paramount objective is to ensure that data is not lost or destroyed.

When operating on an international scale, preserving data requires much more focus. Moreover, the stakes are higher in the context of an FCPA investigation, where corporate executives will try to demonstrate that they had implemented specific measures to monitor compliance and deter the behavior that led to alleged violations. Few things can derail an attempt to cooperate with the government than to disclose that a key suspect’s data was lost at the start

of the investigation.

Therefore, the core component of a CIP, similar to that of an e-discovery data map, is to identify the information sources that may be subject to monitoring or investigation, and to create a process that ensures such data can and will be preserved.

The CIP helps compliance officers or investigators get to the heart of the matter more quickly, thereby limiting potential liability or damage to brand and reputation. Additionally, the plan helps investigators understand the technology options available for document search, analysis and review. As these are continually evolving, the plan should be updated regularly.

A CIP would consider how to handle an investigation that may touch a country in Europe, Asia or South America, where data privacy laws restrict the processing of personal data, whether it is used to monitor for compliance with antibribery rules, or in response to a government inquiry about the same.

To the extent data must be turned over to U.S. agencies, blocking statutes are another concern. Specifically designed to counter the reach of U.S. discovery, these laws prohibit nationals outside the U.S. from disclosing information in response to U.S. discovery requests, even in the face of a subpoena. These statutes can put a respondent in the unenviable position of having to choose between contempt of a U.S. court, or civil and criminal penalties before their own local courts. Such laws should therefore be factored into a company’s CIP program.

Selecting a Data Management/Response Team

Considering these challenges, selecting the right team to handle data collection and analysis is a critical issue. If you are proactively implementing a monitoring plan, you can make deliberate choices to balance the needs of your organization. For example, you could consider creating an in-house task force, drawing from IT and law department resources.

However, relying on in-house resources for investigations is a double-edged sword. The compliance effort could be undermined if the in-house team is perceived as not sufficiently thorough or,

worse, complicit in concealing improper payments. In the Daimler matter, the government deemed that Daimler’s FCPA violations were enabled by “an inadequate compliance structure.” In its information, the government highlighted that Daimler’s internal audit team was aware of bribe payments and the methods use to implement them. In one instance, the internal audit team indicated that a scheme benefited from a low likelihood of detection, albeit at higher cost. Principal Deputy Assistant Attorney General Mythili Raman said in a statement: “[T]hese companies saw foreign bribery as a way of doing business.”

At a more basic level, an external resource can be particularly valuable in identifying the best tools to analyze any transaction. FCPA investigations can require simple financial accounting, a more in-depth analysis of transaction records, or an evaluation of a social network to determine who may have been involved or have known of a specific transaction. Knowledge of specific languages and local rules regarding the processing of data are also important.

Whether dealing proactively or reactively, it is advisable to have third parties involved to avoid the appearance of self-dealing, and to have an impartial party able to credibly testify in court to explain and defend the investigation process.

U.S. regulators have made it abundantly clear that they are intent on investigating corrupt practices wherever they occur to enforce the FCPA. This places a serious compliance requirement on the part of U.S. and foreign corporations that fall under the scope of the FCPA. Other countries’ own enforcement of antibribery laws, such as China’s prosecution against Rio Tinto executives, highlight that enforcement extends beyond U.S. agencies.

For any company concerned about FCPA, a true desire to monitor for compliance is clearly a prerequisite. Additionally, its legal department will need relatively immediate access to the data relevant to such transactions, which will require some amount of proactive work. From a compliance perspective, this access can mean the difference between early identification and resolution — or hearing about it first from one of the agencies. ■