ALM
LAW JOURNAL NEWSLETTERS

The Corporate Counselor®

Volume 21, Number 9 • February 2007

Litigation Readiness

When Is the Right Time to Assess?

By Prashant Dubey

With the amendments to the Federal Rules of Civil Procedure (FRCP), precedent-setting adverse sanctions against some of the largest corporations and growing regulatory requirements, the need to become "litigation ready" has been like a large snowball, gaining mass and momentum. The indisputable need to become litigation ready has arrived, and the snowball continues to get bigger and faster as it heads down the mountain.

With the FRCP amendments, Dec. 1 has come and gone and guess what? Nothing has exploded. Since the amendments were billed as the legal industry's Y2K, all the lather and lament was almost anti-climatic. Does that mean that the amendments to the rules governing discovery are meaningless? Not at all. It simply means that Dec. 1 was an initial deadline for anxieties to manifest in real pain. The pragmatic implications of the amended FRCP are that courts and litigants will START to implement portions of the guidelines in new matters that arise and in current matters that have not yet encountered discovery.

Electronically Stored Information

What does all this mean for improving the business process of responding to discovery when

continued on page 8

The McNulty Memo

The DOJ and the Waiver of the Attorney-Client Privilege

By Steven P. Solow

On Dec. 12, 2006 the U.S. Justice Department issued new guidance that will require federal prosecutors to seek approval from senior DOJ officials before requesting a waiver of attorney-client privilege and work product protection in corporate criminal investigations. The new guidance supersedes the existing language on waiver in the "Thompson memo," issued by then-Deputy Attorney General Larry D. Thompson in January 2003.

The Thompson memo, formally titled "Principles of Federal Prosecution of Business Organizations," provided nine factors for prosecutors to consider when deciding whether to bring criminal charges against a corporation. Included among those factors is a consideration of whether the corporation indicated a "willingness to cooperate" with the investigation by, among other things, disclosing complete results of internal investigations and waiving attorney-client and work product protection.

McNulty Changes

In a speech before a group of lawyers in New York, Deputy Attorney General Paul J. McNulty explained that the new guidance continues to require consideration of the factors from the Thompson memo, but adds new restrictions. Specifically, it requires prosecutors to establish a legitimate need for privileged information and to seek approval before requesting it from the company. To seek privileged attorney-client communications or legal advice, prosecutors must obtain approval directly from the Deputy Attorney General — currently, McNulty. To seek privileged factual information, such as facts uncovered during a company's own internal investigation of misconduct, the prosecutor must seek the approval of the U.S. Attorney in his or her local district who must, in turn, consult with the Assistant Attorney General of the Criminal Division.

According to McNulty, privileged attorney-client communications "should be sought only in rare circumstances." Moreover, if a company decides not to waive privilege, "prosecutors are directed not to consider that declination against the corporation in their charging decisions." The guidelines also instruct prosecutors not to "take into

continued on page 2

In This Issue

McNulty Memo

continued from page 1

account whether a corporation is advancing attorneys' fees to employees or agents under investigation and indictment," except in the "extremely rare case" where the totality of the circumstances shows that the company intended to impede the investigation.

A Step in the Right Direction, But Far Enough?

The response to the Department's sudden change of position by corporate counsels, white-collar practitioners, and Congress appears to be less than enthusiastic. If the goal of the McNulty memo was to provide businesses with a renewed sense of confidence when seeking attorney guidance and counsel in dealing with complex compliance issues, the effort of the Department may have fallen far short.

There should be no doubt that the ultimate goal of the government's policies is to help ensure sound financial markets, safe food and drugs, environmental protection and worker safety. It is a fact that our success in obtaining any of these goals depends on voluntary compliance by regulated businesses. There is little question that even the threat of unrestricted waiver requests chilled the ability of businesses to have legal counsel guide those compliance efforts. The Department itself identifies its policy as an effort to support compliance, which is in effect a recognition that the old policy was hurting efforts to enhance corporate compliance guided by in-house and outside legal counsel and the effective conduct of internal investigations. However, the test for regulated businesses will be how this new guidance is used by the Department. That is, is this truly a new policy, or will it just be a bureaucratic hurdle on the same bad policy path?

Some suggest that McNulty's effort will not resolve the problem in its entirety. They reason that, as long as DOJ is permitted to consider waiver to be an element of cooperation, businesses are still going to have the not-so-subtle pressure to waive privilege, even when it is not specifically asked for by DOJ. In the experience of many white-collar practitioners, companies that have waived privilege in the past few years were never directly asked to do so by DOJ; rather, they proactively chose to do so in order to get cooperation points with DOJ. The solution is to no longer make waiver a consideration in charging decisions, period.

Also disturbing to many is the government's continuing consideration of a company's legal assistance to its employees and directors. The government is left to decide if the company "shield[ed] … culpable employees" during an investigation, and sanction accordingly, placing companies in the untenable position of having to predict whom the government will ultimately determine to be "culpable." For fear of guessing wrong, companies are encouraged to compromise the rights and interests of their employees.

A Government Position in Conflict with Itself?

In his important new book on corporate criminal liability, Professor William Laufer of the Wharton School sees an inherent contradiction in the federal government's policy on corporate criminal cases. In *Corporate Bodies and Guilty Minds*, Professor Laufer observes that the Sentencing Guidelines seek to have corporations "face the threat of significant punishment and, at the same time, the possibility of … leniency … " by providing for significant penalties but mitigating those penalties if, among other things, the company agrees to cooperate with the government's investigation. Similarly, the Thompson memo regarding charging decisions and plea negotiations, urged aggressive prosecution of corporations while at the same time offering leniency or absolution for companies that accept responsibility

continued on page 11

Steven P. Solow is a partner in the Washington office of Hunton & Williams LLP, where he was chief of the Environmental Crimes Section in the Department of Justice from 1997 to 2000. His practice focuses on business crimes, internal investigations, corporate compliance and security programs, and environmental civil and criminal litigation. He can be reached at ssolow@hunton.com.

The Corporate Counselor®

EDITOR-IN-CHIEF . . . . . Adam J. Schlagman
EDITORIAL DIRECTOR . . . . . Wendy Kaplan Ampolsk
MARKETING DIRECTOR . . . . . Colin Graf
MARKETING COORDINATOR . . . . . Beth Ann Montemurro
MARKETING ANALYSIS COORDINATOR . . . . . Traci Footes
GRAPHIC DESIGNER . . . . . Crystal Hanna

The Corporate Counselor® (ISSN 0888-5877) is published by Law Journal Newsletters, a division of ALM.

The Corporate Counselor P0000-233
Periodicals Postage Pending at Philadelphia, PA
POSTMASTER: Send address changes to:
ALM
345 Park Avenue South, New York, NY 10160
Annual Subscription: $365

Published Monthly by:
Law Journal Newsletters
1617 JFK Boulevard, Suite 1750, Philadelphia, PA 19103
www.ljnonline.com

Title VII Disparate Pay Claims

A Possible Flood?

By Debra S. Friedman

The U.S. Supreme Court is currently considering a case of great importance to employers, *Ledbetter v. Goodyear Tire & Rubber Co., Inc.* It will decide when the statute of limitations begins to run under Title VII of the Civil Rights Act of 1964 (as amended) ("Title VII") for certain types of disparate pay claims.

Most employers have compensation systems that are non-discriminatory on their face. However, even a lawfully designed system can be used as a tool for intentional discrimination if the evaluator misuses the process. *Ledbett*er presents the issue of whether the statutory clock begins to run when an employer utilizing a lawfully designed compensation system makes an allegedly illegal pay decision or whether the clock runs anew each time an employer issues a paycheck reflecting the allegedly discriminatory pay decision. The result will impact an employer's potential liability for intentional pay discrimination under Title VII.

Title VII

Under Title VII, employees have 180 days from the date of an alleged violation to file a discrimination charge with the Equal Employment Opportunity Commission (EEOC) if they work in a state that does not have a state or local administrative agency authorized to remedy violations. If an employee works in a state with such an agency, the employee must file a charge within 300 days of an alleged Title VII violation. Therefore, the battle is over how to apply Title VII's short statute of limitations period.

Ledbetter's Path to the U.S. Supreme Court

Lilly Ledbetter, a former area manager at a Goodyear Tire plant in Alabama, sued her employer under Title VII, alleging she received lower pay than her male counterparts as a result of sex discrimination. Ledbetter waited until after she retired from Goodyear Tire to sue, claiming she received paychecks within the 180-day statutory period that were the result of discriminatory pay decisions. Notably, those pay decisions were all based on annual salary reviews made prior to the applicable 180-day statutory period, and covered her 19-year career at the plant. Ledbetter sued in Alabama federal district court in 1999, claiming sex discrimination, age discrimination and retaliation under several federal statutes. Only her Title VII claims proceeded to trial. On the disparate pay claim, the jury was permitted to consider pay decisions dating back to 1979 because Ledbetter's 1998 paychecks reflected all the pay decisions made during the course of her employment. The jury returned a verdict favoring Ledbetter on her disparate pay claim, awarding damages exceeding $3.8 million dollars — later reduced to $360,000, plus attorneys' fees and costs.

Goodyear appealed. The Eleventh Circuit Court of Appeals reversed, finding that pay claims are discrete acts. It held that the statute of limitations ran from the date the employer made the pay decision, not from the date the employer issued a paycheck reflecting the pay decision. Accordingly, the appeals court only considered Goodyear's 1997 and 1998 pay decisions, based on written performance evaluations, and found no evidence of sex discrimination.

The Eleventh Circuit went on to state that, in disparate pay cases where the employer has a system for periodically reviewing and re-establishing employee pay, an employee may reach outside the limitations period no further than the last pay decision immediately preceding the start of the limitations period. The court then added it was not holding that an employee may reach back to the last pay decision preceding the start of the limitations period, only that an employee may reach back no further. Ledbetter petitioned the U.S. Supreme Court for review. The Court granted certiorari in June 2006.

Where to Draw the Line on the Statute of Limitations

Prior court precedent and policy considerations play a major role in *Ledbetter*. In *Amtrak v. Morgan*, 536 U.S. 101 (2002), the Supreme Court held that the limitations period under Title VII begins to run when an employer commits a discrete act of discrimination. Goodyear Tire argues there is no basis for treating pay decisions differently than other discrete acts. Goodyear also points to Supreme Court cases arguing that events occurring outside the limitations period, but whose effects are presently felt, are nothing more than unfortunate events in history with no present legal consequences.

Ledbetter and employee groups counter by pointing to cases such as *Bazemore v. Friday*, 478 U.S. 385 (1986) for support, noting that receipt of each paycheck can be actionable under Title VII. Goodyear Tire and employers have tried to limit *Bazemore* to its facts, as it involved a discriminatory pay structure rather than a facially neutral compensation system.

On the policy side, the struggle is between the competing interests of employees, who face illegal pay discrimination in perpetuity if they do not promptly challenge an initial discriminatory decision, and employers who wish to avoid stale claims. Employees argue that they do not always know they are victims of discrimination given the often hidden nature of compensation systems.

The Potential Impact on Employers

If Goodyear Tire prevails in *Ledbetter,* employers can rely on the certainty associated with statutes of limitation; they will not be required to defend against stale claims of disparate pay. Employers therefore can focus on ensuring that current pay practices are

continued on page 4

Debra S. Friedman is a member of Cozen O'Connor, practicing in the Labor & Employment Practice Group in Philadelphia. She has 14 years of experience in litigating and counseling employers, including Fortune 500 and Fortune 100 companies, on discrimination claims. Friedman has served as a lecturer in *National Railroad Passenger Corp. (Amtrak) v. Morgan* — a case that could play a prominent role in *Ledbetter*. She may be reached at dfriedman@cozen.com.

Pay Claims

continued from page 3

non-discriminatory, avoiding the need to revisit all pay decisions made during an employee's career.

If Ledbetter wins, however, the potential fallout for employers is significant. Management may have to defend against a slew of disparate pay claims going back years. They may also need to seriously consider retaining documents for the course of an employee's career, or longer in certain instances, to access evidence they may need at a later date. Other potential obstacles are out of employers' control: mobility of the workforce, deceased or otherwise unavailable witnesses, faded memories and lost or destroyed documentation.

The Value of a Solid Performance Evaluation System

One of the key lessons to be learned from *Ledbetter*, regardless of its outcome, is that employers must pay attention to their performance evaluation systems — frequently used to determined wage decisions. It is true that no reasonable amount of monitoring guarantees employers will pick up every bias that may have influenced an employee's evaluation years ago. Nevertheless, employers can and should take certain steps to minimize their risk exposure to disparate wage claims.

Design a Facially Neutral System. This is the place to head off most problems. Take a fresh look at your performance evaluation system, in addition to verifying all evaluative criteria are job-related. Determine if they accurately reflect an employee's job functions and, where appropriate, compliance with important company policies such as equal employment opportunity (EEO) laws, workplace safety and attendance/tardiness. The bottom line is that evaluation criteria must not be premised on unlawful considerations of gender, race, national origin, religion, age, disability or any other protected status. If any unlawful bias is found, management must promptly correct pay disparities for those adversely affected by unlawful considerations. Many, if not most, performance evaluation systems today will pass the threshold test of facial neutrality — just like the system in *Ledbetter*. Therefore, the focus will be implementing and monitoring the performance evaluation system.

Train Evaluators. Often, the people doing the evaluating either do not understand how to do a proper evaluation or they let their biases influence the process. As a result, the breakdown in performance evaluation systems frequently occurs. Effective training of evaluators can reduce this risk. As a starting point, evaluators should be people familiar with the employee's job duties and actual performance. This is necessary for a meaningful evaluation, but also focuses the evaluator on job content and reduces conscious and/or unconscious bias. Also, management should institute formal training for evaluators, including the role of EEO laws and awareness of unlawful biases potentially influencing the evaluation process. To be effective, the training should highlight unlawful factors that cannot play a role, such as sex, race, national origin, religion, age, disability or any other protected status. It's vital to recognize the impact of unduly harsh or lenient evaluations, as they can open the door for bias or, at the every least, the perception of bias. Also emphasize the focus on performance, not personality. Finally, caution evaluators about the potential exposure that results when evaluators "take the easy way out" by rating poor performers as satisfactory to avoid confrontation.

Require Next-Level Management Review. Checks and balances are key to successfully implementing a performance evaluation system. Perhaps the quickest way to catch any bias is requiring that the evaluator's manager review all evaluations. The manager can ensure evaluations are based on objective data where possible and that subjective portions are free from any apparent unlawful bias. Accordingly, this tier of managers should also receive formal training on the proper way to do performance evaluations.

Specify the Reason for Each Wage Adjustment. While no system is perfect, linking merit-based wage adjustments to performance evaluations provides a visible, written and hopefully objective basis for the decisions. Wage adjustments also may be linked, from time to time, to market conditions. For instance, an employer may raise the wages of employees with more longevity to equal the wages of newer employees who were able to command higher wages due to market conditions, as opposed to experience. Management should document these adjustments separately from merit-based adjustments. Companies also should advise employees of the basis for all wage adjustments, including cost-of-living modifications. Good communication is necessary to avoid the appearance that a particular wage adjustment is in recognition of superior performance—especially if the employee's performance is only average.

Communicate with the Employee Under Evaluation. Communication is critical in all employee relations matters, and the performance evaluation process is no exception. Companies should provide employees with advance notice of employer's expectations and evaluation criteria, and then sit down with each employee and go over the evaluation. Employees also should be given an opportunity to comment on their evaluations. Effective communication here promotes understanding between management and the employee. While it does not guarantee that employees will agree with their evaluations, open communication does reduce the likelihood that an employee will view the evaluation process as unlawful.

Monitor the System. Evaluators and reviewers will come and go, and some are more critical of employees than others. Accordingly, management should have a means of monitoring their performance evaluation system at yet another level, both on a yearly basis and over time. Higher-level management or human resources managers can provide this additional check — another way to capture and correct any bias potentially influencing evaluations and consequently wage decisions. It also educates the administration about how the performance evaluation system is being implemented.

continued on page 12

Compliance with Non-U.S. Environmental Health and Safety Regulations

Potential Pitfalls for U.S.-Based Companies

By Steven M. Siros

Most U.S.-based companies have fairly sophisticated environmental, health and safety ("EHS") programs that are designed to ensure compliance with applicable EHS rules and regulations. The reasons for such programs are obvious: EHS compliance represents the floor for most, if not all companies, and non-compliant companies are likely to experience adverse financial, environmental, health and safety impacts as a result of non-compliance.

In order to be compliant, companies obviously must be able to identify applicable EHS rules and regulations. Although companies' EHS programs are generally well designed to identify applicable U.S. rules and regulations, these programs may overlook non-U.S. EHS laws and regulations that can also can impact U.S.-based companies' ability to market products not only abroad, but in the United States as well. An example of such "overlooked" rules and regulations may be recent EHS directives/regulations promulgated by the European Union (the "EU") and its individual "Member States."

EU 'Directives'

Over the past several years, the EU has implemented a number of EHS "Directives," which regulate products that are sold (either directly or indirectly) in the EU. The most significant of these Directives (from an EHS perspective) are: 1) the Restriction of Hazardous Substance Directive ("RoHS"); 2) the Waste Electrical and Electronic Equipment Directive ("WEEE"); and 3) the Registration, Evaluation and Authorization of Chemicals Directive ("REACH") (The latter is actually a "regulation," which means that it applies directly and uniformly across all member states, unlike a "directive," which must be integrated by each member state into its existing regulatory scheme). As is further discussed below, companies whose EHS programs fail to proactively identify and develop compliance strategies for these and other EHS rules and regulations are likely to quickly find themselves at a competitive disadvantage and may in fact find themselves unable to sell products in certain markets.

RoHS

The RoHS directive applies to specific types of electric and electronic equipment ("EEE") that is sold in the EU. The RoHS directive, which became effective on July 6, 2006, regulates the following categories of EEE: 1) large household appliances (*i.e.*, washing machines, refrigerators, etc.); 2) small household appliances (*i.e.*, vacuum cleaners, toasters, etc.); 3) computer and telecommunication equipment (*i.e.*, products and equipment for the collection, storage, processing, presentation or communication of information by electronic means and products or equipment for transmitters, sound, images, or other information by telecommunications); 4) lighting equipment; 5) electrical tools (*i.e.*, saws, drills); 6) toys; and 7) automatic dispensers (*i.e.*, vending equipment). Subject to certain exemptions, any EEE sold in the EU that falls into one of these seven categories must now be free of lead, mercury, cadmium, hexavalent chromium, poly brominated biphenyls and poly brominated diphenyl ethers. EEE that contains any of these prohibited substances cannot be sold in any EU member state.

The RoHS exemptions are somewhat fluid as new exemption requests are filed by regulated industries on a fairly frequent basis. Currently, regulated EEE that is utilized for the protection of the security interests of an EU member state is, not surprisingly, exempt from the RoHS requirements. Exemptions are also provided for certain lead alloys and mercury that is contained in florescent and other lighting equipment (This is not an exhaustive list; manufacturers of regulated EEE are encouraged to evaluate the current exemption list to determine whether any other RoHS exemptions might apply). Companies which manufacture regulated EEE need to ensure that their EHS professionals stay abreast of these changing exemptions.

WEEE

The WEEE directive also regulates EEE; in fact, WEEE applies to the same categories of EEE as RoHS, as well as two additional categories, medical monitoring devices and control equipment. Manufacturers and importers of these EEE products are required to set up and/or fund a collection and disposal program to ensure proper management of these EEE products at the end of their useful life. The WEEE directive is similar to regulations currently being promulgated in a number of states such as California and Oregon.

Producers of regulated EEE are required to register in each member state and identify the volume of regulated EEE placed on the market. For EEE placed on the market after August 13, 2005, producers are responsible for participating in a system (either individually or collectively) for the collection and disposal of those products. With respect to historical EEE (*i.e.*, EEE that was placed on the market prior to Aug. 13, 2005), current producers are required to contribute to the costs that are being, and will be, incurred to dispose of these historical products based on the producer's current market share. There are a number of financing mechanisms which have been put into place to enable producers to meet their WEEE obligations, including blocked bank accounts, insurance products, or participation in a collective industry group.

For U.S.-based companies, the WEEE directive poses unique challenges. At the present time, only producers, importers, and exporters based in the EU are able to register. Although

continued on page 6

Steven M. Siros is a partner in Jenner & Block's Chicago office. He is a member of the Firm's Environmental, Energy and Natural Resources Law, Insurance Litigation and Counseling, and Products Liability and Mass Tort Defense Practices, focusing his practice on both litigation and regulatory matters. He may be reached at ssiros@jenner.com.

Non-U.S. Regulations

continued from page 5

U.S.-based companies cannot market non-compliant products in the EU, those companies currently cannot register their products as required by WEEE. U.S.-based companies are thus required to affiliate themselves with an EU-based importer who then is responsible for WEEE compliance.

Again, just as with the RoHS directive, companies that manufacture products in the U.S. for export into the EU will be unable to market those products unless the products are WEEE compliant, and companies that have failed to proactively identify the WEEE requirements will be at a competitive disadvantage until they are able take the necessary steps to affiliate with an EU-based importer and comply with these requirements.

REACH

The REACH regulation is similar to the Toxic Substances Control Act in the United States, and will apply to chemical manufacturers in the EU beginning on June 1, 2007. REACH is designed to streamline the existing legislative framework governing the production and importation of chemical substances in the EU. REACH is intended to create a single system to regulate "new" and "existing" chemical substances, and is expected to spur the phase-out of more dangerous chemicals in favor of safer substitutes.

REACH will require manufacturers and importers of chemical substances in the EU to submit registrations for every chemical that is manufactured or imported in a quantity greater than one metric ton per year. The information to be included in the registration depends on the volume of chemical produced. For chemical substances produced in amounts between one and ten tons, a technical dossier containing information on the properties, uses, and classification of the chemical is required. Chemical substances produced in excess of ten tons will require a chemical safety report that documents the hazards and classification of a particular substance, as well as an assessment of the risks associated with the particular chemical.

In addition, for chemicals that are deemed to pose high risks to health or the environment, chemical manufacturers will be required to evaluate whether lower risk substitute products exist; if lower risk products do exist, the manufacturers will be required to phase-out the more harmful substance. If no lower risk alternative exists, the manufacturer will be obligated to submit a research and development plan which documents the efforts the manufacturer will undertake to find a safer substitute chemical.

Just as with WEEE, in order for U.S.-based companies to export chemical substances into the EU, the U.S.-based company will need to partner with an EU-based importer (or appoint an "only representative") who will be responsible for complying with the REACH requirements. Non-REACH compliant chemical substances will not be able to be marketed and/or imported in the EU after June 1, 2007.

Implications of Newly Promulgated EHS Regulations

For U.S.-based companies that produce and sell EEE and chemical products in the EU, these directives/regulations should have been on the EHS radar screens many months ago, and compliance strategies should have already been developed and implemented. If these directives/regulations were not previously identified, immediate efforts should be undertaken to develop a compliance strategy to address these new regulations. However, these are just examples of the types of regulations that can impact U.S.-based companies. There are many less publicized EHS rules and regulations promulgated by the EU and other countries on a frequent basis. For example, China is in the process of developing its own versions of RoHS and WEEE that will affect products being imported/exported from China. Many other countries are also evaluating whether to promulgate similar regulations.

As such, companies need to ensure that their EHS programs are designed to proactively identify these new rules and regulations to enable necessary product and/or process modifications to be made in a timely manner. Active participation in trade groups and review of environmental publications are excellent mechanisms for keeping abreast of EHS developments abroad. Again, the focus must be on proactively identifying these potentially applicable regulations before they are promulgated because once the regulation is promulgated, it is often too late as it takes time to modify the product or process, and companies may find themselves in a position of being unable to produce and/or sell their products until the modification is complete.

Finally, it is important to note that these EHS directives do not only affect companies that produce and market their products outside of the United States. Companies that produce and market products in the United States may be affected as well. For example, many companies are finding that even their U.S.-based customers are demanding that electronics be RoHS compliant so that those electronics can be integrated into products that are later sold in the EU. In other instances, companies which rely on parts or components which are manufactured in the EU may find that these components have been modified in order to meet the RoHS and WEEE requirements which may result in the parts or components no longer being suitable for their intended use. Similarly, chemical manufacturers in the EU may elect or be forced to cease production of certain chemical products as a result of the REACH regulations. U.S.-based companies that rely upon those chemicals will need to seek alternative suppliers (at a potentially higher price) or modify the manufacturing process to utilize a less hazardous alternate chemical.

For many years, the EHS regulations in the United States had set the bar. Now, however, many countries are promulgating EHS regulations that go beyond the U.S. regulations. It is therefore no longer sufficient for U.S.-based companies to be solely focused on compliance with U.S. laws and regulations without considering the implications of non-U.S. EHS regulations. Companies need to ensure that their EHS compliance systems are properly designed to proactively identify these new EHS rules and regulations in sufficient time to enable any necessary modifications to be made such that a company's products can continue to be sold in the United States and abroad.

—❖—

Voluntary Disclosures of Export Violations

By Robert Clifton Burns

The recent settlement agreement entered in the EP MedSystems matter (described below) does little to refute the common wisdom that the Depart-ment of Commerce's Bureau of Indus-try and Security ("BIS") treats voluntary disclosures of export violations more harshly than other agencies that regulate exports from the United States. It also illustrates a potential, but avoidable, peril in the two-step voluntary disclosure process urged by BIS and other federal agencies. Finally, it serves as yet another example of the regulatory minefield that U.S. export laws present for U.S. companies with foreign subsidiaries.

Unlicensed Shipments to Iraq

At issue are six shipments of seven items of heart monitor equipment valued at $510,590. The equipment was shipped by EP MedSystems from its subsidiaries and/or distributors in Germany, the Netherlands and the United Kingdom to Iran between March 2001 and April 2004 without a license. Shipments of these devices to Iran after July 26, 2001 would have been permissible, notwithstanding the U.S. sanctions on Iran, under the Trade Sanctions Reform Act of 2000 provided that a license had been obtained. Five of the six shipments in question occurred after that date and without a license. The company agreed to settle the charges by BIS for payment of a fine of $244,000. (As will be more fully described below, BIS was not the only federal agency investigating these shipments!)

The company filed two voluntary disclosures with BIS relating to the shipments. The first was a preliminary disclosure that was filed on Oct. 13, 2003, approximately two weeks after one of the shipments at issue had taken place. The second was a final disclosure that the company filed on Nov. 20, 2003. This followed a common procedure, also encouraged by BIS, to file an initial preliminary disclosure upon discovery of a violation and then a final, and more complete, disclosure after the Company has had an opportunity to fully investigate the violation at issue.

Normally, it would have been a significant mitigating factor that most of the shipments described in the voluntary disclosure would have been routinely granted a license if an application had been filed. In such a case, the violation is more a technical violation than the substantive violation that would occur when the shipment is made in a circumstance where the exporter would have been unlikely to obtain a license. BIS, however, paid no attention to that factor and, instead, focused on alleged misrepresentations in the voluntary disclosures themselves. The evidence supplied in the charging letter for each of these violations is, charitably, not terribly overwhelming.

Alleged Misrepresentations in The Voluntary Disclosures

Four false statements in the preliminary and final voluntary disclosures were alleged by BIS. The first was the claim in the Oct. 13 preliminary disclosure that the Company filed the disclosure "immediately" after learning of the shipments to Iran. The charging letter alleged that this was false because the company first learned of the shipments based on one email dated May 22, 2003, between unnamed EP Med-Systems officials A five-month delay is, perhaps, not immediate, but it hardly seems a sufficient justification for a significant fine for misrepresentation. Moreover, it may well have been the case that the Company had not yet discovered the May email or other earlier documents when it filed the preliminary disclosure in October.

Second, the charging letter took issue with the claim in the initial Oct. 13 voluntary disclosure that the company did not know before Oct. 2003 about the exports to Iran. This claim is also based on that single e-mail in May 2003 between unidentified company officials and which the company may not have discovered at the time of the preliminary disclosure.

The third false statement pointed to in the charging letter allegedly occurred in the final version of the voluntary disclosure filed on Nov. 20. According to the BIS charging letter:

> In its disclosure, EP MedSystems stated that it "has no record of ever having sold any of its products to any customer in Iran." This statement, representation or certification is false or misleading because, at the time it was made, EP MedSystems had in its possession a number of documents indicating that the company had sold its products to Iran. These documents include an email between EP Med-Systems officials dated on or about May 22, 2003, which listed five hospitals that were operating EP MedSystems equipment.

This is a confusing allegation since the preliminary voluntary disclosure made by the Company on Oct. 13 appears to have indicated and admitted that the Company had such records. Indeed, how could the Company have made either the preliminary voluntary disclosure or the final one without such records? Here it looks like BIS's charge either takes the sentence in question out of context or deliberately misreads it.

Fourth and finally, the BIS charging letter attacks a statement in the final voluntary disclosure that its European Sales Manager was "totally unfamiliar with the U.S. Government restrictions on exports to Iran." This statement was false, according to BIS, because the European Sales Manager "had been informed of the U.S. embargo of Iran and knew that certain equipment required a license for export to Iran." Again, BIS seems intent on stretching the likely meaning of the voluntary disclosure to find a misrepresentation in it. What was likely meant by the disclosure was not that the sales manager didn't know that the U.S. forbade shipments to Iran. Rather, it seems likely that the company was truthfully representing that the sales manager didn't know that U.S. export law could be violated by a shipment of goods from a non-U.S. distributor or subsidiary. Although there can be such a violation for such a re-export of U.S. origin goods, it would not be surprising for

continued on page 8

Robert Clifton Burns is a partner at Powell Goldstein LLP in Washington, DC, and an Adjunct Professor of Law at the Georgetown Law Center. He can be reached at 202.624.3949 or cburns@pogolaw.com. He also is the editor of, and a contributor to, Export-LawBlog (www.exportlawblog.com).

Export Violations

continued from page 7

employees of overseas subsidiaries or distributors to not be aware of this.

LESSONS TO BE LEARNED

So what lessons should be taken away from this? First, companies should be aware that filing a voluntary disclosure of illegal exports with BIS can lead to substantial civil penalties. Here this occurred because BIS used alleged misrepresentations in the disclosures as the basis for the penalty, but substantial penalties can follow a voluntary disclosure even where misrepresentations are not alleged. In May 2006, BIS and Ingersoll-Rand agreed to a $680,000 fine after Ingersoll-Rand filed a voluntary disclosure. In the same month, BIS and UGS Corporation agreed to a $57,750 fine for $43,257 in exports that were voluntarily disclosed to BIS.

In response to this criticism (which this author first made in a blog posting in December), Wendy Wysong, Deputy Assistant Secretary of Export Enforcement at BIS, wrote an article, titled "BIS Data Show Benefits of Voluntary Self-Disclosure," which appeared in the December issue of *The Export Practitioner*. Ms. Wysong argued that in only a handful of cases arising from voluntary self-disclosures did BIS impose (through settlement or otherwise) a fine in excess of 50% of the maximum fine that could be imposed. That argument, while facially persuasive of certain benefits, completely neglects BIS's admitted practice of charging multiple violations for each individual export, thereby significantly inflating the maximum fine.

While these considerations might legitimately deter certain exporters from filing a voluntary disclosure with BIS relating to exports that they otherwise feel might not be subsequently discovered by BIS, there are certainly instances where some exporters might file voluntary disclosures notwithstanding any impending fear of harsh treatment. For example, publicly traded companies will have Sarbanes-Oxley disclosure obligations that will make public disclosure of the violations necessary. Additionally, many companies may legitimately fear that export violations will be uncovered in due diligence investigations conducted in connection with sale of the company

continued on page 12

Litigation Readiness

continued from page 1

compelled to produce Electronically Stored Information (ESI)? It means that there is never a bad time to get started on business process improvement, even if a company is in the midst of litigation. This process improvement needs to begin with assessment as you can't really know where you are going if you don't know where you are.

There are three approaches a litigation readiness assessment (LRA) can take:

Retrospective

Some corporations, when describing their "as-is" discovery response process, use a most recent matter as the basis for their LRA responses. In some cases, the discussion specifically refers to "who did what to whom" on that particular matter. This can be a very useful approach since the information is fresh in peoples' minds and there is likely some documentation, like actual letters of preservation or litigation hold notices, which can be called upon to illustrate actual practices. Furthermore the pain that was inevitably encountered during the process (or lack thereof) is real and tangible, so the assessment is not an academic, abstract exercise.

Abstract

This approach assumes that the company will be sued and compelled to produce ESI. This amounts to a mock electronic discovery response process. An LRA conducted in this mode can be valuable because participants can truly feel proactive rather than feel their actions will be viewed under a microscope or that they will be inadvertently (or deliberately) be made into scapegoats on a recent matter. They can take charge of the process without hesitation and without the threat of being judged by their colleagues.

Active

Tying an LRA to an active matter can be one of the most effective approaches. One very pragmatic reason is that it may be possible to pay for the LRA with matter-specific funds. This could be really important to the general counsel that may not have discretionary budgets. Additionally the recommendations of the assessment can be applied immediately to the existing matter and be used to support strategy and tactics with privilege applied.

In a real-case example, one corporation had asked its electronic discovery services provider to help it prepare for its Rule 26(f) "meet and confer" conference, as well as help it complete a rational Form 35 submission for a particular "bet-the-company" lawsuit. In addition, the client wanted to use the learning from the provider's work to help improve its overall process for electronic discovery response, independent of this particular matter. As the work commenced, the team was able to gather data on which data repositories were accessible, inaccessible and defensible; use the information to support the 26(f) preparations; and make a value judgment on the elegance (or lack thereof) of the company's processes. Another benefit of this approach was that it was easier to get resources from multiple disciplines to take the time to respond to the interviews and data gathering overtures, since this truly was a "bet-the-company" lawsuit.

CONCLUSION

Ultimately, assessment is always a good idea. Corporations that take the time to understand exactly where they are can develop a baseline from which to target process improvements, prioritize more rationally what to work on first, and demonstrate to interested parties that they are truly making a good-faith effort to improve their processes. As the scenarios above illustrate, there is never a bad time to assess.

—❖—

Prashant Dubey is Vice President and General Manager of Fios' Discovery Management Services consulting group. He has consulted with Fortune 250 corporations for more than 20 years on business process optimization, cost management and performance management.

Where Privacy and Corporate Governance Laws Meet

Information Security Obligations

By Melissa J. Krasnow

[Editor's Note: This is the first in a series of articles addressing some of the key issues surrounding corporate responsibility with respect to the privacy of information and security breaches.]

As business information, particularly in electronic format, continues to proliferate, the need to maintain the security of this information is increasing. There are privacy and corporate governance laws that govern the obligation of a company to keep information secure. According to the Global State of Information Security 2006, a worldwide study by CIO magazine, CSO magazine and PricewaterhouseCoopers representing the responses of almost 7800 senior executives, "Noncompliance runs broad and deep in all industries, and ignorance of applicable law is a big factor." This article provides an overview of two important information security obligations — security procedures and practices and document destruction — under privacy and corporate governance laws.

SECURITY PROCEDURES AND PRACTICES

State Security Procedures and Practices Laws

A few states have enacted laws regarding a company's duty to maintain reasonable security procedures and practices. Arkansas, California, Nevada, Rhode Island, and Texas and Utah enacted security procedures and practices laws. California was the first state to enact a security procedures law. Under the California law, a company that owns or licenses personal information about a California resident must implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification or disclosure.

Personal information means an individual's first name or first initial and last name in combination with any of the following data elements, when either the name or data elements are not encrypted: 1) Social Security number; 2) driver's license number or state identification card number; 3) account number, credit card number or debit card number in combination with any required security code, access code or password (e.g., a PIN) that would permit access to an individual's financial account or (iv) medical information.

Federal Trade Commission Security Procedures Standards

Although there is no specific federal security procedures law for all companies, the Federal Trade Commission has described standards for security procedures in a number of recent cases. By way of example, in the BJ's Wholesale Club case in 2005, the FTC charged that BJ's failure to provide reasonable security for sensitive customer information was an unfair act or practice in violation of Section 5 of the Federal Trade Commission Act because it caused substantial injury that was not reasonably avoidable by consumers and not outweighed by offsetting benefits to consumers or competition. The FTC alleged that BJ's: 1) failed to encrypt consumer information when it was transmitted or stored; 2) stored the information longer than it had a need to do so; 3) stored the information in files that could be accessed using commonly known default user IDs and passwords; 4) failed to use readily available security measures to prevent unauthorized wireless connections to its networks; and 5) failed to use measures sufficient to detect unauthorized access to the networks. The settlement order for this case requires BJ's to establish and maintain a comprehensive information security program that includes administrative, technical and physical safeguards and to obtain regular third party professional audits of this program for compliance with the FTC Order and with book-keeping and record-keeping requirements. The FTC Order is in effect for a 20-year period.

Sarbanes-Oxley Act

Pursuant to Section 404 of the Sarbanes-Oxley Act of 2002 (SOX), management of a public company is responsible for establishing and maintaining adequate internal control over its financial reporting. Management must evaluate and report on the effectiveness of internal control over financial reporting in the annual report filed by a public company with the Securities and Exchange Commission. This management report is accompanied by an attestation from the independent auditor of the public company. Management also must evaluate and disclose changes that have materially affected or are reasonably likely to materially affect a public company's internal control over financial reporting in the quarterly and annual reports. Moreover, the Chief Executive Officer and Chief Financial Officer of a public company must provide certifications regarding their responsibility for establishing and maintaining internal control over financial reporting and the design of internal control over financial reporting to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. These certifications are attached as exhibits to a public company's quarterly and annual reports.

In re Caremark

This suit against the board of directors of Caremark International Inc. involved claims that the directors breached their fiduciary duty of care to the company in connection with alleged violations by Caremark employees of state and federal laws. *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del.Ch. 1996). The plaintiffs sought to recover losses on behalf of the company from the directors. According to the Delaware Chancery Court:

> [I]t is important that the board exercise a good faith judgment that the corporation's information

continued on page 10

Melissa J. Krasnow is a partner in the Corporate Group of Dorsey & Whitney LLP (e-mail: krasnow.melissa@dorsey.com).

Privacy

continued from page 9

> and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility . . . [A] director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards.

DOCUMENT DESTRUCTION

State Document Destruction Laws

Close to one-third of states have enacted laws requiring the destruction of documents. Arkansas, California, Hawaii, Indiana, Kansas, Kentucky, Montana, Nevada, New Jersey, North Carolina, Rhode Island, Tennessee, Texas, Utah, Vermont and Washington enacted document destruction laws. Under the California law, a company must take all reasonable steps to destroy or arrange for the destruction of the records of a customer within its custody or control containing personal information which is no longer to be retained by: 1) shredding, 2) erasing, or 3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

Personal information means any information that identifies, relates to, describes or is capable of being associated with, a particular individual, including: 1) name; 2) signature; 3) Social Security number; 4) physical characteristics or description; 5) address; 6) telephone number; 7) passport number; 8) driver's license or state identification card number; 9) insurance policy number; 10) education; 11) employment; 12) employment history; 13) bank account number; 14) credit card number; 15) debit card number or 16) any other financial information. "Records" refers to any material regardless of the physical form on which information is recorded or preserved by any means (*e.g.*, in written or spoken words, graphically depicted, printed or electromagnetically transmitted).

Fair and Accurate Credit Transactions Act

The Disposal Rule under the Fair and Accurate Credit Transactions Act of 2003 (FACTA) requires a company that maintains or otherwise possesses consumer information for a business purpose to properly dispose of consumer information by taking reasonable measures to protect against unauthorized acquisition or use of the information in connection with its disposal. Consumer information means any record about an individual in paper, electronic or other form that is derived from a consumer report or a compilation of such record. Disposal refers to the discarding or abandonment of consumer information or the sale, donation or transfer of any medium (including computer equipment) upon which consumer information is stored.

Reasonable measures include establishing and complying with policies to: 1) burn, pulverize or shred papers containing consumer report information so that the information cannot be read or reconstructed; 2) destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed; and 3) conduct due diligence and hire a document destruction contractor or dispose of material specifically identified as consumer report information. Although the FACTA Disposal Rule applies to consumer reports and the information derived therefrom, the FTC, which enforces this Rule, encourages those that dispose of any records containing a consumer's personal or financial information to take similar protective measures.

SOX

Two sections under SOX that cover document destruction apply to a company, whether public or private. Section 802 of the Sarbanes-Oxley Act states:

> [W]hoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined … imprisoned not more than 20 years, or both.

Section 1102 of SOX states in pertinent part:

> [W]hoever corruptly … alters, destroys, mutilates, or conceals a record, document, or other object, or attempts to do so, with the intent to impair the object's integrity or availability for use in an official proceeding; or … otherwise obstructs, influences, or impedes any official proceeding, or attempts to do so … shall be fined … or imprisoned not more than 20 years, or both.

CONCLUSION

As information security obligations are continually changing, the laws governing information security obligations are evolving. Laws in different areas like privacy and corporate governance are both addressing these obligations. As a result, a company must carefully and constantly monitor developments in all of these laws in order to comply with them. According to the Ernst & Young 2006 Global Information Security Survey, compliance requirements in the past year have most significantly impacted and in the next year likely will continue to significantly impact the information security practices of companies.

Next month, the author will outline the requirements for providing notification of a security breach under state security breach notification law by any company and the factors that a public company needs to take into account regarding whether to disclose a security breach under federal securities law.

—❖—

McNulty Memo

continued from page 2

and do so by agreeing to cooperate with the government's investigation.

Professor Laufer believes that, in the circumstances of today, these twin approaches of prosecution and punishment for past acts, and leniency for subsequent cooperative behavior, undermine the use of criminal liability as "the ultimate lever that empowers less formal social controls, such as self-regulation … " Whether or not one agrees with this analysis, there is no question that the government's policy of conditioning leniency on cooperation led to a battle between the Department of Justice and a remarkable coalition of business and civil liberties groups opposed to the provisions of the Sentencing Guidelines and the Thompson memo that made waiver of the attorney-client privilege a measure of cooperation.

On April 5, 2006, the Sentencing Commission voted to remove the language from the corporate sentencing guidelines that identified waiver of the attorney-client privilege as a part of meaningful cooperation with a government investigation or prosecution. The Commission did so in the face of opposition to this change by the Department of Justice.

INSIDE BASEBALL

So what changed and led to DOJ's abrupt reversal? The turnabout has been labeled a "lesson in how to construct a model lobbying effort," by *Legal Times* [a sister publication of this newsletter]. The efforts brought together unlikely allies, including the American Bar Association, the American Civil Liberties Union, the American Chemistry Council and the Association of Corporation Counsel.

These groups joined an advocacy avalanche that included the Conference of Chief Justices and a letter from former DOJ officials from different administrations who usually only come together at funerals. In the words of the former Justice officials (contained in a Sept. 5, 2006 letter to Attorney General Alberto Gonzales) the Department's position on waiver of attorney-client privilege was "seriously flawed"; they urged the Department to revise its policy to "state affirmatively that waiver of the attorney-client privilege or work-product protections should not be a factor in determining whether a company has cooperated with the government in an investigation."

But perhaps the signal moment came during a House of Representatives hearing when Associate Attorney General Robert D. McCallum sought to defend the Department's position at a House Judiciary subcommittee meeting on March 7, 2006. In attendance were Reps. William Delahunt (D-MA) and Dan Lungren (R-CA), generally polar opposites on almost every issue. As Associate Attorney General, McCallum was seeking to defend the department's position, Representative Delahunt interjected the following:

Mr. Delahunt: … And, you know, I think that you can probably sense by the questions that have been posed, as well as observations by individual Members, that there is a real concern here. And you don't want someone like Lungren from California, you know a far-right conservative Republican, and Delahunt, this Northeast liberal, filing legislation on this because I think that is the order of magnitude that is being expressed here. So respectfully, that is a message that I think you can bring back to Justice, is that there is concern about the Thompson/McCallum Memorandum. Okay?

Mr. McCallum: I will certainty take that message back, Mr. Delahunt.

Then, in September 2006, Reps. Lungren and Delahunt published an Op-Ed in *The Hill,* in which they asked the Department of Justice to "not consider any company or other entity to be 'non-cooperative' for protecting its right to consult confidentially with its attorneys," and said that if they "refuse to do so, Congress should act."

Shortly prior to the adjournment of the 109th Congress, Sen. Arlen Specter (R-PA), the outgoing chairman of the Senate Judiciary Committee, introduced legislation designed to protect the attorney-client privilege by broadly prohibiting prosecutors from determining that a target is not cooperating with a government investigation based on a valid assertion of privilege. While the bill had no chance of passing before the end of the term, it did serve as a warning that Congress was prepared to act. A mere five days later, the McNulty memo was issued by the department.

WILL CONGRESS STILL ACT?

The McNulty revisions to the Thompson memo seem to have done little to assuage congressional concerns. On Jan. 4, Specter reintroduced his bill (S. 186), the Attorney-Client Privilege Protection Act of 2007. The bill amends Title 18 of the U.S. Code by adding a new section, § 3014, prohibiting any agent or attorney of the U.S. government in any criminal or civil case to demand, request or condition treatment on the disclosure of any communication protected by the attorney-client privilege or attorney work product. Nor can charges or treatment be conditioned on whether the organization pays attorneys' fees for its employees or signs a joint defense agreement.

In a statement on the Senate floor, Specter thanked the Department for its effort in issuing revisions to the Thompson memo, but declared that effort insufficient. "The new memorandum is inadequate in its protection of the attorney-client privilege," he said. He acknowledged that the McNulty memo "makes some improvements," but added that "the revision continues to erode the attorney-client relationship by allowing prosecutors to request privileged information backed by the hammer of prosecution if the request is denied."

Specter said his bill was designed to "force the Department of Justice to issue a meaningful change to its corporate charging policies beyond the changes in the McNulty Memorandum, which came 'a day late and a dollar short.'" The memo, he said, "continues to threaten the viability of the attorney-client privilege in business organizations by allowing prosecutors to request privilege waiver upon a finding of 'legitimate need' — a standard that should guide the most basic of prosecutorial requests, not sensitive requests for privileged information."

The Senator was also critical of the memo for discouraging corporate

continued on page 12

McNulty Memo

continued from page 11

employees from having frank discussions with lawyers in furtherance of compliance efforts. "The Department of Justice will not prevent corporate misconduct if it continues to inadvertently discourage the types of internal investigations and dialogues corporate officials need to detect and prevent corporate fraud," he said.

As a former prosecutor, Specter said he was "acutely aware of the enormous power and tools a prosecutor has at his or her disposal," even without "the coercive tools of the privilege waiver" as embodied in the McNulty memo. "Cases should be prosecuted based on their merits, not based on how well an organization works with the prosecutor," he remarked.

—❖—

Pay Claims

continued from page 4

While adding this additional step is clearly time-consuming, a spot check of evaluations generally is the realistic way to approach monitoring. Those involved should focus on consistency within job categories and among similar types of jobs, and then compare wage decisions, promotions, demotions and transfers tied to performance evaluations.

CONCLUSION

Hopefully, the U.S. Supreme Court in *Ledbetter* will recognize workplace realities and follow prior Supreme Court precedent, holding that employers cannot be held liable for the current effects of past discriminatory pay decisions. In the meantime, while there's certainly no magic wand for removing all bias from the performance evaluation process, especially going back in time, employers can remain focused on reducing their risk exposure. The key is being proactive in managing the process.

—❖—

Export Violations

continued from page 8

that committed the violations.

Once a company decides that a voluntary disclosure is prudent, then there is a very clear lesson to be taken away from the EP MedSystems case. Obviously, everything that is said in a voluntary disclosure must be accurate or the company risks further fines based on claims of misrepresentation. Most importantly, companies should be particularly careful about statements made in the preliminary disclosure made to the agency prior to a full investigation of the violations discovered. The purpose of the preliminary disclosure is simply to inform the agency of the violations so as to receive any potential mitigation allowed under the rules. Nothing else should be in that disclosure. In other words, the preliminary disclosure should be short and sweet, saying only that the company has discovered that it shipped product X to country Y on Z date without a license and that the company will provide a full disclosure of the facts surrounding these exports after it has completed its internal investigation. It should not use the preliminary disclosure to start building its case by stating that there were no other exports, that the exports were immediately reported, that the persons made a mistake of law, etc.

EP MedSystems also illustrates that a company's export compliance efforts cannot stop at the borders of the U.S. The exports that resulted in the fine were made by non-U.S. employees or distributors of the Company. It seems reasonable to suppose that they did not consider that U.S. export restrictions to Iran would apply to their own exports from Europe to Iran. EP MedSystems might have avoided this entire debacle with a little bit of export training for its overseas staff.

If there are any readers who are thinking that a $244,000 fine, while unpleasant, is not catastrophic, you should understand that the costs, both actual and potential, to EP MedSystems substantially exceed that number. In the company's latest 10-Q, the company reveals that it is subject to an SEC investigation arising out of statements it made in its SEC filings relating to the exports. Additionally, the company discloses that it has incurred almost $1,000,000 in legal fees to date arising out of its efforts to defend itself from charges arising from the export. In addition to the SEC and BIS investigations, there was a criminal export investigation by the U.S. Attorney's office, which was dropped. There is a pending investigation by the Department of Treasury's Office of Foreign Assets Control ("OFAC") arising from EP MedSystem's violation of OFAC rules through its receipt of funds from Iran as a result of the exports.

PAYING THE ULTIMATE PRICE

Finally, the President, CEO and COO of the Company, Reinhard Schmidt, was terminated by the Board for cause because of his certification of the statements made in the voluntary disclosures to BIS.

—❖—