

Decisive Win for the Defense

In a unanimous decision, the US Supreme Court sided with the defense in *Dura Pharmaceuticals Inc. v. Broudo*. In one of the most anticipated management liability cases of 2005, the court addressed how damages are to be calculated in securities fraud cases. The Court held that investors suing a corporation and its directors and officers will have to show a link (, a causal connection) between alleged illegal activity and the drop in stock price. Previously, California's Ninth Circuit allowed a looser standard, which arguably served to inflate the plaintiffs' damage assessments. In at least some Ninth Circuit cases, the Supreme Court's decision will most likely result in lower settlements (partial wins) and the filing of motions to dismiss and/or summary judgment motions (potentially total wins for the defendants). At the very least, it will put plaintiffs under pressure to justify their damage calculations.

Dura Case Background

The company's stock was at \$53 a share when it made allegedly false high claims about the firm's success. The stock later dropped to \$9.75 and the company announced that one of its products had not won approval from the Food and Drug Administration. The shareholders brought an action for fraud, stating that certain company executives had fraudulently misrepresented the company's prospects to the market as a whole. The interesting fact here, however, is that the stock had actually dropped *prior to* the company's announcement; after the disclosure, the stock price remained flat.

Prior to this decision, the Eighth and Ninth Circuits had allowed plaintiffs to sue for damages where a company's alleged misrepresentations merely "touched upon" the

reasons for the subsequent stock drop, without having to prove that they were causally related. Stocks move up and down for various reasons, not merely due to securities fraud. Allowing plaintiffs to attempt recovery of the entire difference between the pre-disclosure high price and the post-disclosure low potentially served to unfairly inflate the value of some securities suits. Now, the burden is clearly on the shareholders to prove that any drop in stock price was directly caused by the fraudulent misstatements.

While the outcome of this case was no surprise, a reverse decision (always a possibility) would have had enormous implications for future Directors & Officers (D&O) settlements.

Now, the burden is clearly on the shareholders to prove that any drop in stock price was directly caused by the fraudulent misstatements.

Another Win for Public Companies – The Krim Case

A recent ruling by the Fifth US Circuit Court of Appeals in *Jerry Krim, et al. v. pcOrder.com Inc.* represented another win for companies sued by shareholders. This case involved losses arising from allegedly false registration statements accompanying public offerings.

In a first-of-its-kind ruling by a federal court of appeals, the Fifth Circuit panel unanimously held that shareholders who purchase shares of company stock after the shares mix in the market with shares from other sources cannot rely on statistical probabilities to establish Section 11 standing to sue over a public offering. In the opinion, the panel focused on



Contents

Decisive Win for the Defense	1
The Watchdog Who Barked Too Late	2
The Rules They Are a-Changing	3
New Federal Rules on Privacy Breaches	3
Arthur Andersen Redux	4
Contacts	4

the requirement that shareholders complaining of false registration statements must be able to trace the shares they bought directly to the challenged offering. Section 11 addresses civil liabilities resulting from false registration statements under the Securities Act of 1933.

In 2003, the Fifth Circuit held in *Rozenzweig v. Azurix Corp.* that after-market stock purchasers do not inevitably lack standing to sue under Section 11 but must demonstrate the ability to "trace" their shares to the prospectus they allege is defective. *Rozenzweig* left unanswered the question of what is necessary to trace shares to the defective prospectus when shares enter the market by means other than the public offering. **The Fifth Circuit answered that question in *Krim*.**

The Fifth Circuit recognized that present market realities may render Section 11 "ineffective as a practical matter" in some instances in which stock is purchased outside a public offering. The court maintained that this is an issue for Congress to address, stating, "It is not within our purview to rewrite the statute to take account of changed conditions." If accepted by the other federal circuits, this decision could have a widespread impact on securities suits relating to initial public offerings.



The Watchdog Who Barked Too Late

Lessons Learned from the SEC's Early Failure to Detect Mutual Fund Trading Infractions

A recent report from the Government Accountability Office (GAO) focused on lessons to be learned from the Securities & Exchange Commission (SEC)'s delay in detecting trading lapses in mutual funds. The report was commissioned in response to

concerns about potential widespread abuses in which mutual fund companies' investment advisers entered into undisclosed arrangements with favored customers, permitting market timing (frequent trading to profit from short-term pricing discrepancies), sometimes in violation of stated trading limits.

Unlike late trading, which is illegal under all circumstances, market timing is not in itself illegal. It is, however, potentially harmful to long-term mutual fund shareholders, because it increases transaction costs while it lowers fund returns. When practiced in violation of fund policies and undisclosed, this kind of trading may constitute illegal conduct. After the practice was identified, industry observers wondered why the SEC, as the mutual fund industry's primary regulator, was so tardy in pursuing these lapses. By the time the SEC took notice and performed its own survey, the Commission estimated that roughly 50 percent of the 80 largest mutual fund companies had entered into undisclosed market timing arrangements in contravention of established fund policies.

Conclusions of the GAO

The GAO report concluded that the SEC didn't look for market timing activity because it considered other activities of greater risk, and because it believed that the mutual fund companies themselves had a financial incentive to control frequent trading, since such activity could reduce fund returns, thereby making a fund less competitive. The report further stated, and the SEC has agreed, that routine assessments of the effectiveness of compliance officers and compliance reports would be necessary to prevent similar problems in the future.

Spotlight on Compliance

This emphasis on compliance officers is significant. Notably, the GAO study found that "in the majority of cases" reviewed, internal fund compliance staff had detected the undisclosed market timing arrangement with favored customers but did not possess the authority within their organizations to correct the situation. In response, the SEC recently adopted a new rule requiring that registered investment companies (mutual funds) and investment advisers each appoint a Chief Compliance Officer (CCO). The CCO of the mutual fund is to report directly to the fund's board of directors. Where the mutual fund itself does not have any employees, the CCO of the investment adviser is to serve the same function. Further, compliance officers are now required to prepare annual reports on the state of their companies' compliance with relevant laws and regulations.

What's Next?

The SEC has created and is staffing a new office to better anticipate, identify and manage emerging risks and market

trends. It has also established a revised set of examination guidelines over potentially high-risk compliance areas (the implementation of which will be assessed in a future GAO study). In response to the information about market timing, the SEC moved aggressively to determine the scope and seriousness of the practice, and then initiated numerous enforcement actions to deter and penalize violators. Similar enforcement reviews and some legal actions followed in several other countries.

The Rules They Are a-Changing

UK Rules of Indemnification

If shielding personal liability is one of the chief reasons corporations are formed, then the details of corporate indemnification are a crucial matter. As such, these details can be found in the local laws governing the formation of a corporation. Typically, the laws permit corporate indemnification to expand in response to increasing personal liability. So it was not so much a surprise as a return to the status quo when the UK recently enacted new legislation to ensure this expansion. The Companies (Audit, Investigations and Community Enterprise) Act of 2004 relaxed a 20-year-old prohibition against corporate indemnification of directors and officers. Formerly, any provision in any contract or company article that attempted to exempt or indemnify any corporate executive from liability arising from negligence, default or breach of fiduciary duty was void under Section 310 of the Companies Act of 1985.

As of April 2005, a UK company *may* legally indemnify its directors against liabilities to “qualifying” third parties (such as creditors, investors and employees). The ban, however, still exists with regard to fines imposed on directors in criminal proceedings, penalties resulting from regulatory infractions, and defense expenses associated with criminal actions where the director was convicted or in any civil action brought by the company itself. This last group may include direct actions by the company as well as those brought derivatively by stakeholders on behalf of the company.

In Synch with Delaware

UK law now more closely approximates that of Delaware’s well-known statutes of indemnification. The new act specifically confirms the continuing right of a company to purchase D&O insurance for the benefit of its directors. Note that “officers” are no longer covered by either the 1985 or 2004 Companies Acts, and that the decision to indemnify these executives is now left to the discretion of the boards of the individual organizations.

This change is likely not the last. With the spotlight still shining on the potential personal exposure faced by corporate executives

globally, we expect that companies will begin or continue reviewing their indemnification provisions on a multinational basis.

New Federal Rules on Privacy Breaches

Companies, healthcare providers and third-party service providers have obligations relating to the privacy of certain protected information collected while implementing employer-sponsored benefit plans. Strict security and confidentiality regulations were passed as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). With a spate of privacy breaches recently making the news, federal regulators have released new guidance about the rules requiring plan sponsors and business associates to report breaches of security covering patient medical information.



The guidance comes from the Centers for Medicare and Medicaid Services at the US Department of Health and Human Services (HHS). It was prompted by concerns from corporate plan sponsors, healthcare providers and the providers’ business associates that HIPAA’s directive to monitor and report security incidents could be overwhelming due to the breadth of the definition of “security incident” under HIPAA: *the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.*

The new guidance suggests using a third-party service contract and/or an employer’s plan document to detail the specific

security incident reporting requirements that should be developed to meet each plan's specific needs. Questions to consider include:

- What specific actions would be considered security incidents?
- How should security incidents be documented and reported?
- What information should be included in reports?
- How often should security incidents be reported?
- What are the appropriate responses to certain security incidents?
- Is identifying patterns of attempted security incidents reasonable and appropriate?

Note: According to HHS, reporting requirements, whether in contracts with healthcare providers' business associates or the plan documents of member employers, must specify that all security breaches need to be reported.

Arthur Andersen Redux

A case currently before the US Supreme Court has the attention not only of many lawyers, both in-house and in private practice, but many accountants as well. In *Arthur Andersen*, now on the Willis CaseWatch, the justices appeared skeptical of the Justice Department's case during oral arguments. In 2002, under a witness-tampering law, a jury found the now-defunct firm guilty of wrongly persuading employees handling the Enron account to engage in massive document destruction, just as federal regulators were beginning to scrutinize the energy trading company's accounting problems in 2001. The issue currently before the Supreme Court relates to the judge's jury instructions in the 2002 trial – instructions which the defense argues unfairly stacked the proceedings against the firm. To convict the firm, the judge explained, the jury had to find that the firm corruptly impeded the fact-finding capability of an official proceeding.

In another action, Andersen's former top Enron auditor was criminally charged for his role in shredding documents after Enron's collapse. He pleaded guilty three years ago to obstruction, and testified in the firm's trial. He remains free as he cooperates with prosecutors.

A successful outcome in their Supreme Court fight may help shield the former partners at Andersen in both present and possible future litigation. This case has garnered such close attention because virtually every company has a document retention program, and every sizeable legal and accounting firm has a client who is a target or potential target of investigation. Stay tuned.

Executive Risks Regional Contacts

For further information, please contact any of the following:

Paul Wendler
One Glenlake
1 Glenlake Parkway, 11th floor
Atlanta, GA 30328
P- 404 224 5123
F- 404 229 4849
paul.wendler@willis.com

Steve Pincus
7 Hanover Square
7th Floor
New York, NY 10004
P- 212 837 0734
F- 212 509 4912
steve.pincus@willis.com

Tom Ciano
Three Copley Place
Suite 300
Boston, MA 02116
P- 617 351 7517
F- 617 351 7430
tom.ciano@willis.com

Todd Jones
5 Corporate Center
100 Matsonford Road
Radnor, PA 19087
P- 610 254 7284
F- 610 254 5600
todd.jones@willis.com

Brian Gauen
10 South LaSalle Street
Suite 3000
Chicago, IL 60603
P- 312 621 4855
F- 312 621 6870
brian.gauen@willis.com

Brenda Shelly
One Bush Street
San Francisco, CA 94104
P 415 291 1520
F- 415 398 4986
brenda.shelly@willis.com

Dan Vecchio
10 South LaSalle Street
Suite 3000
Chicago, IL 60603
P- 312 621 4799
F- 312 621 6870
dan.vecchio@willis.com

Guy Dodson
One Camomile Street
London EC3A 7LA
United Kingdom
P +44 (0) 20 7975 2800
F +44 (0) 20 7975 2584
dobsong@willis.com

Jim Iacino
1400 16th Street
Suite 400
Denver, CO 80202
P- 720 932 8203
F- 720 932 8138
jim.iacino@willis.com