June 27, 2006

While decisions of the Supreme Court are widely publicized, the actions of state legislatures which impose affirmative obligations on employers often pass with less fanfare or notice. In either case, however, the effect on employers may be profound. The first part of this News Alert summarizes the recent decision of the Supreme Court in Burlington Northern & Santa Fe Railway Co. v. White which will make it easier for plaintiffs to pursue retaliation claims under Title VII. The second part covers the recent trend in state laws covering incidents of data breach. These laws generally require employers to notify employees if there has been unauthorized access to their personal information kept by the employer. Failure to comply with state data breach statutes may result in significant fines, up to $10,000 per day per violation.

Supreme Court Expands Retaliation Standard Under Title VII

On June 22, 2006, the Supreme Court clarified the proper standard for evaluating retaliation claims under Title VII in a unanimous decision in Burlington Northern & Santa Fe Railway Co. v. White, No. 05-259. The Supreme Court articulated a broader, albeit objective, test for retaliation which will make it easier for plaintiffs to bring retaliation claims for a wider variety of actions by an employer. Plaintiffs need not show that an employer's actions were employment-related to prove their retaliation complaint. A plaintiff may make a cognizable retaliation claim by showing that the employer took action which caused a material harm and which would dissuade a reasonable employee from making or supporting a charge of discrimination.

The anti-retaliation provision of Title VII of the Civil Rights Act of 1964 forbids an employer from "discriminating against" an employee or job applicant because that individual "opposed any practice" made unlawful by Title VII or "made a charge, testified, assisted, or participated in" a Title VII proceeding or investigation.

Sheila White was the only female forklift operator in her department at Burlington's Tennessee yard in June 1997. In September of 1997 White complained of being harassed by her supervisor. Burlington suspended her supervisor, but then removed White from forklift operations and assigned her to less desirable track laborer tasks. In October, White filed a complaint with the Equal Employment Opportunity Commission ("EEOC") claiming that her reassignment was unlawful gender-based discrimination and retaliation for having complained about her supervisor. She filed another complaint with the EEOC in December. Shortly thereafter, White was suspended without pay for insubordination after a dispute with her supervisor. Following an internal investigation, Burlington found that White had not been insubordinate, reinstated her and awarded her backpay for the 37 days she was suspended. White then filed her Title VII action, claiming that Burlington's actions of reassigning her to another position and suspending her without pay amounted to unlawful retaliation. The jury found for White, awarding her $43,500 in compensatory damages. The Court of Appeals for the Sixth Circuit panel reversed. The Sixth Circuit sitting *en banc* later affirmed the jury's verdict on White's retaliation claims.

Prior to the Supreme Court's decision in Burlington Northern, the federal circuit courts used different standards of proof for retaliation claims. Several circuits required that plaintiff must have suffered at least some materially adverse employment action, such as a loss of compensation, benefits or opportunities for promotion. The Supreme Court concluded that Congress intended Title VII's anti-retaliation provision to sweep more broadly than the anti-discrimination provision, which only applies to employment opportunities and status, and the terms and conditions of employment. Justice Breyer, writing for the Court, agreed with the Seventh and District of Columbia Circuits' approach, finding actions to be retaliatory "if materially adverse, which in this context means it might well have dissuaded a reasonable worker from making or supporting a charge of discrimination." The Court emphasized the reasonable employee standard as a judicially administrable, objective standard, and one necessary to separate significant from trivial harms. Justice Breyer explained for the majority that the Court used general terms to articulate the standard because "any given act of retaliation will often depend upon the particular circumstances."

Applying this standard, the Court held that the jury had a reasonable basis to find that both White's reassignment and her suspension were material harms. Even though White's job title and job description did not change, there was evidence that her re-assignment to track duties from the forklift tasks was a harder, dirtier and less desirable job. The suspension was similarly material despite the fact that the employer later rescinded the suspension and paid White backpay for the time lost. The court wrote that "many reasonable employees would find a month without a paycheck to be a serious hardship." The Court reasoned that both of these actions were likely to dissuade a reasonable employee from opposing discrimination or bringing a discrimination claim, and thus affirmed the *en banc* Sixth Circuit's decision.

The Court's broader retaliation test allows employees who have opposed discrimination, or filed EEOC charges, to bring retaliation claims for adverse actions that are likely to dissuade a reasonable employee from objecting to discrimination. Faced with this broader exposure to liability, employers may want to take additional steps to limit the risk of retaliation claims, such as providing additional training to supervisors and human resources personnel, or to monitor closely actions that are adverse to employees who raise discrimination complaints. Once retaliation claims are asserted, it is likely to be more difficult for an employer to obtain summary judgment with regard to whether a reasonable employee would be dissuaded by the employer's actions, at least until the courts have sufficient experience in making those determinations. Thus, the Supreme Court's decision in Burlington Northern will likely continue the trend over the past several years of significantly increasing numbers of retaliation claims.

States Expand Data-Breach Notification Laws

Within the past three months, six states—Hawaii, Vermont, New Hampshire, Indiana, Wisconsin, and Nebraska—have passed data-breach notification statutes that differ in several significant respects from similar older laws that impact when and how employers across the country must disclose data-security breaches.

Over the past four years, a total of 33 states (see table below) and the territory of Puerto Rico have enacted statutes requiring companies to disclose when a security breach of personal information occurs. Most of these statutes have the same basic requirement: If an unauthorized person acquires or accesses an employee's personal information, the company must alert the employee about the security breach.

Some statutes also require the company to notify state consumer protection agencies, law enforcement agencies and the credit reporting agencies—Equifax, Transunion, and Experian—if the security breach involves a large number of people (usually 500 or 1,000 employees).

Although penalties for non-compliance vary under each statute, several states impose fines as high as $10,000 *per day* of violation. Thus, a failure to notify employees for a month could lead to staggering liability.

Beyond SSNs

The majority of state data-security notification statutes apply only to electronic data that include employees' names and either their social security numbers, driver's license numbers, or financial account numbers (for example, a checking account or direct deposit number).

But some of the newer laws—Nebraska's statute, approved on April 6, 2006, and Wisconsin's statute, approved on March 16, 2006—expand protected information to include "biometric data"—a term that encompasses such things as fingerprints and voiceprints.

In addition to protecting electronic files, Hawaii's statute applies to instances in which an unauthorized individual acquires an employee's paper records.

Across state lines

Most state statutes require companies doing business within the state to notify only that state's residents of a security breach. As a result, if a company with offices in California and Oregon, for example, has a security breach involving the employment records of residents from both states, California's notification statute would require alerting only California employees. Oregon does not have a notification statute, so the company need not notify its Oregon employees.

In contrast, Wisconsin's new statute requires companies based in Wisconsin to notify *all* their employees whose information is affected regardless of where those employees live or work. Similarly New Hampshire's new law requires any company doing business within New Hampshire to notify all of its employees whose information is affected by a security breach.

Most state statutes also apply only to companies that are doing business within the state. But Indiana's and Hawaii's new laws purport to apply to any company (inside or outside of those two states) that has "personal information" about the state's residents. Consequently, if your company has offices only in Illinois, but has even one employee who is a resident of Indiana, Indiana's statute would apply. As a practical matter, however, it is not clear that these statutes' extra-territorial scope would withstand judicial challenge.

Calling up the authorities

Before notifying an employee concerning a security breach, employers should review, or have their attorney review, the applicable notification statutes. A few such laws—including New Hampshire and Hawaii's new statutes—require the employer, in addition to notifying the employee, to notify government agencies such as the state attorney general's office, or the state department of consumer protection.

Although some statutes do not require notifying employees of a breach if the company determines that misuse of employees' information is unlikely or not possible, they still may require notification of state agencies.

For example, suppose employment records are inadvertently e-mailed to someone outside the company, but a company representative is able to contact the recipient and obtain evidence that the records were never opened. Vermont's new statute may allow the company to forego alerting its employees of the possible breach, but would require the company instead to provide state agencies with details about the incident and the company's investigation.

What to do if a breach occurs

It is helpful for a company to develop a written policy on how to deal with a data-security breach before it happens. Caught unprepared, an organization might find by the time it has determined that a particular state's statute applies, it already has violated some of the law's provisions and possibly incurred thousands of dollars in penalties.

A breach notification policy should take into account all state notification laws that *might* apply, not just the laws of the state in which the company is located. Generally such a policy should provide for taking the following steps in the event of a data-security breach:

- Notify counsel as soon as possible. A legal opinion often is necessary to identify all the data-security breach statutes that apply, especially if the company has offices in more than one state, does business with clients in more than one state, or has employees from more than one state. If selecting an outside attorney, look for one with prior experience with state data-security laws. That may or may not be the company's usual labor and employment counsel.

- Immediately initiate an investigation to evaluate the threat of harm to employees.

- If there is reason to believe that the incident could possibly result in the misuse of information, notify—with counsel—any necessary governmental agencies. This includes appropriate law enforcement agencies, who may want to investigate the individual that obtained the personal information. It also may include state agencies that must be notified before you can notify employees of the breach.

- If there is no reason to believe that the incident will result in the misuse of information, many states will not require notification of employees. If notification is not required, prepare a written document describing the scope and findings of your investigation. Some states may require maintaining this document for at least five years, others may require providing it to a state agency.

- If notification is required, accomplish it as soon as possible. In any event, notification should occur within 45 days.

It is doubtful that the latest round of state notification statutes will be the last. Other states are considering similar statutes, and Congress is considering over a half a dozen federal data breach notification proposals. This much is certain—failing to act quickly when there is a breach in the security of employee records can come at a high price for a company and for its employees.

States That Have Enacted Breach Notification Statutes

State	Enacted	State	Enacted
Arizona	2006	Nebraska	2006
Arkansas	2005	Nevada	2005
California	2002	New Hampshire	2006
Colorado	2006	New Jersey	2005
Connecticut	2005	New York	2005

Delaware	**2005**	**North Carolina**	**2005**
Florida	**2005**	**North Dakota**	**2005**
Georgia	**2005**	**Ohio**	**2006**
Hawaii	**2006**	**Pennsylvania**	**2005**
Idaho	**2006**	**Puerto Rico**	**2005**
Illinois	**2005**	**Rhode Island**	**2006**
Indiana	**2006**	**Tennessee**	**2005**
Kansas	**2005**	**Texas**	**2005**
Louisiana	**2005**	**Utah**	**2006**
Maine	**2005**	**Vermont**	**2006**
Minnesota	**2006**	**Washington**	**2005**
Montana	**2006**	**Wisconsin**	**2006**

The above article was written by David Zetoony, Bryan Cave lawyer working out of the firm's Phoenix and Washington, D.C., offices. It was published by the Society for Human Resource Management in its online news on June 22, 2006.

* * * * * * * * *

Labor and Employment Practice – Contact Information

Chicago Office
161 North Clark, Chicago, IL 60601
Jules I. Crystal (312) 602-5065
Jackie V. Iannicelli (312) 602-5134
Timothy C. Klenk (312) 602-5008
Mary Margaret Moore (312) 602-5090
Rodney Perry (312) 602-5160
Christy E. Phanthavong (312) 602-5185
Christian M. Poland (312) 602-5085
Wendy J. Smith (312) 602-5023
James M. Staulcup, Jr. (312) 602-5055
William J. Wortel (312) 602-5105

Irvine Office
2020 Main Street, Suite 600, Irvine, CA 92614
Sean D. Muntz (949) 223-7274
Julie E. Patterson (949) 223-7144

Kansas City Office
3500 One Kansas City Place, Kansas City, MO 64105-2100
Beth Romans Bower (816) 391-7663
W. Perry Brandt (816) 374-3206
Karen K. Cain (816) 374-3356
Jennifer A. Donnelli (816) 292-7841
Heather S. Esau Zerger (816) 374-3357
Rick E. Frawley (816) 374-3427
Robert J. Hoffman (816) 374-3229
Elaine D. Koch (816) 374-3235
Catesby A. Major (816) 374-3339
Lynn S. McCreary (816) 374-3208
Tarun Mehta (816) 374-3269
Jeremiah J. Morgan (816) 391-7647
Kelly Messing Nash (816) 374-3236
Meredith J. Rund (816) 374-3320
Stacy O. Schorgl (816) 374-7604
Sarah N. Swatosh (816) 374-3334
Julie Westcott (816) 374-3204
Ronnie B. Winfrey (816) 391-7609

London Office
33 Cannon Street, London, England EC4M 5TE
Sarah Linton (011) 44-20-7246-5935
Edward W. Wanambwa (011) 44-20-7246-5842

Los Angeles Office
120 Broadway, Suite 300, Santa Monica, CA 90401-2305
Howard O. Boltz (310) 576-2233
Pamela C. Calvet (310) 576-2390
Kaye E. Chaffee (310) 576-2293
Amy M. Gantvoort (310) 576-2379
Leslie H. Helmer (310) 576-2218
Jamie L. Johnson (310) 576-2121
Agatha M. Melamed (310) 576-2129
David H. Raizman (310) 576-2120
Harry R. Stang (310) 576-2241
Lynn K. Thompson (310) 576-2344

New York Office
1290 Avenue of the Americas, New York, NY 10104-3300
Vincent Alfieri (Group Leader) (212) 541-2270
Elizabeth Bousquette (212) 541-1251
Christine Cesare (212) 541-1228
Kyle P. Flaherty (212) 541-2134
Dennis Fleischmann (212) 541-1215
Matthew K. Fleming (212) 541-3004
Ruth L. Friedman (212) 541-1137
James F. Gill (212) 541-2222
Elizabeth J. Goldberg (212) 541-2262
Hope Sarah Goldstein (212) 541-1168
William J. Hibsher (212) 541-1085
Zachary A. Hummel (212) 541-1158
David P. Kasakove (212) 541-2096
Norman K. Samnick (212) 541-1146
Steven M. Stimell (212) 541-2042
Dermot J. Sullivan (212) 541-2135
Herbert Teitelbaum (212) 541-1083
Brian J. Turoff (212) 541-3169
Jay P. Warren (212) 541-2110

Phoenix Office
1 Renaissance Square, Phoenix, AZ 85004-4406
Kyle S. Hirsch (602) 364-7170
Caroline K. Larsen (602) 364-7371
Catherine M. Lockard (602) 364-7294
Kira D. Lodge (602) 364-7125

St. Louis Office
One Metropolitan Square, St. Louis, MO 63102-2750
Hollye S. Atwood (314) 259-2334
Ellen E. Bonacorsi (314) 259-2804
Michael P. Burke (314) 259-2700
Elizabeth C. Carver (314) 259-2121
Dennis C. Donnelly (314) 259-2325
Heidi K. Durr (314) 259-2476
Veronica A. Gioia (314) 259-2932
Laura R. Giokas (314) 259-2153
Jerry M. Hunter (314) 259-2772
Charles B. Jellinek (314) 259-2138
Charles A. Lawrence, Jr. (314) 259-2279
Ned O. Lemkemeier (314) 259-2111
Gregg M. Lemley (314) 259-2793
Lisa Demet Martin (314) 259-2125
Timothy C. Mooney (314) 259-2374
Daniel M. O'Keefe (314) 259-2179
Sara E. O'Keefe (314) 259-2727
Nakeyia S. Williams (314) 259-2383

Washington Office
700 13th Street, N.W., Washington, DC 20005
Stacey Ormsby (202) 508-6134
Daniel I. Prywes (202) 508-6094