



## Liability for employee identity theft is growing

[HR Magazine](#) , [June, 2005](#) by [Diane Cadrain](#)

A group of Michigan employees recently broke new legal ground when a jury awarded them \$275,000 for the disasters that befell their lives when their union neglected to safeguard their Social Security and driver's license numbers. The verdict against Michigan Council 25 of the American Federation of State, County, and Municipal Employees (AFSCME) is the first in the nation to find that a custodian of employee information has a duty to guard the data with scrupulous care.

As reports of high-profile security breaches across the country continue to escalate, and the number of victims burgeons, many experts think that, with the Michigan case as a benchmark, courts across the nation are poised to find employers liable for the consequences of their failures to keep personal data private. And in the state capitols, lawmakers are starting to create new duties for employers, making them responsible for safeguarding sensitive information. Here's a look at what's going on in the courts and the state legislatures.

"The Michigan case is the first I've seen that affirms the imposition of liability on the person who negligently handled sensitive information," says attorney Philip Gordon of law firm Littler Mendelson. "It's a national precedent that opens the door to employer liability for workplace identity theft in other jurisdictions that likely will follow Michigan's example."

"We know that identity theft is escalating," says Judith Collins, director of the Michigan State University-Business Identity Theft Partnerships in Prevention, suggesting that more decisions like Michigan's are waiting to happen. "Our phones are ringing off the hook. And we know that the majority of identity thefts happen in the workplace," said Collins.

According to David Parker of law firm Charfoos and Christensen, who represented the Michigan employees, the situation occurred because officials of Michigan Council 25 of AFSCME allowed their union secretary, Yvonne Berry, to take work home, including lists of the Social Security numbers, dates of birth and driver's license information of emergency service operators working for the City of Detroit. Berry's daughter, Dentry Berry, gained access to the employee data at the home, went on a spending spree and brought havoc to the lives of 13 public employees.

"When the charges started rolling in, for almost two years, these people had to spend hours of their days, every day, dealing with angry creditors," Parker said. "One person had to postpone her retirement because her credit had been trashed. Another couldn't get credit at a time when she needed it badly.

Another had to deal with an angry wife who looked at the charges and was convinced that he'd set up housekeeping with a honey." The jury award compensated them for the mental anguish of trying to straighten out their credit histories.

Eric Frankie, who represented Michigan Council 25 of AFSCME in this lawsuit, did not return phone calls.

Why should HR be on the hook? As a central repository of employee data, HR is particularly vulnerable to potential security breaches. "All aspects of the traditional HR function, from recruitment, to selection, to socializing employees to the company culture, to rewarding employees for safeguarding security, are outdated because they don't incorporate security into every aspect," Collins says.

What to do:

- \* Develop uniform, industrywide standards for managing the threat of identity theft to customers, employees and the business itself.

- \* Eliminate the use of Social Security numbers and set up an employee identification number system.

- \* Consider implementing policies that inform employees of their rights and the company's policies. In doing so, Gordon says, employers should go beyond the bare requirements of the law. For example, "employers should detail how [documents] should properly be destroyed."

DIANE CADRAIN, J.D., IS A FREELANCE WRITER IN WEST HARTFORD, CONN.