

01/19/2006

Identity Theft: Limiting Your Employees' Risk -- And Your Liability

By Peter Marshall

The problem of identity theft continues to grow in severity, both in terms of frequency and associated costs. With the workplace ranking as the number one source of identity theft, and with new laws that expose companies to fines and lawsuits for such thefts, employers should consider offering identity theft protection as an employee benefit.

In 2004, 9.3 million Americans--or one in every 25 adults--were victims of identity theft, according to a report by the Better Business Bureau and Javelin Research. The Federal Trade Commission (FTC) estimated that identity theft crimes tallied \$52.6 billion in fraud that year, or almost \$200 for every man, woman, and child in the U.S. Identity theft has been the fastest growing crime in the US for the past three years, according to the FTC, which predicts that in five years, the majority of Americans will have been victimized by identity theft.

Identity theft wreaks significant damage on its victims. The most recent figures from the Identity Theft Resource Center (ITRC), which conducts extensive research and reporting on such crimes, are that out-of-pocket expenses related to identity theft have risen to \$1,495, up from \$808 in 2002, plus \$16,000 in average lost wages.

The average time it takes victims to recover from identity theft has risen to 607 hours, up from 175 hours in 2002. While personal liability is low in the majority of cases, a survey for Nationwide Insurance showed that 16 percent of victims were forced to pay an average of \$6,440 to cover thieves' purchases. And perhaps the greatest impact is long-term, as victims remain vulnerable for the rest of their lives. The ITRC reports that identity thieves are likely to use stolen data months or years later.

In 2005, there were at least 104 serious "data incidents" in the U.S. that compromised the records of more than 56.2 million people. And the New York Times reported last year that a worldwide criminal identity marketplace has now matured, with credit card numbers, Social Security numbers, and other personal data commonly traded and sold in huge numbers.

Employers Have A Major Stake

The number one underlying source of identity fraud is theft of employer records. A Michigan State University study found that 51 percent of all identity thefts occur in the workplace, usually perpetrated by people hired to perform low-level tasks, such as data entry.

While many businesses are most fearful for the security of their client records, payroll records are more often what's stolen, and with increasing frequency. About 90 percent of business record thefts involve payroll or employment records; only about 10 percent involve customer lists, according to the FTC.

On June 1, 2005, a new provision of the Fair and Accurate Credit Transactions Act (FACTA) took effect. It states that any employer whose action or inaction results in the loss of employee information can be fined by federal and state government, and sued in civil court. An employee is entitled to recover actual damages sustained if their identity is stolen due to the employer's inaction, or statutory damages up to \$1,000. Employees may also bring class-action suits against employers for actual and punitive damages. In addition, federal fines of up to \$2,500 per employee, and state fines of up to \$1,000 per employee also may be levied.

A recent case in Michigan highlights another source of corporate liability. In the 2005 case of Audrey Bell et al vs. AFSME AFL-CIO Local 1023, the Michigan Appeals Court affirmed a jury award of \$275,000 to AFSME members who had sued the union for failing to safeguard its members' Social Security numbers. It recognized a special relationship between the union and its employees, including a duty to protect them from identity theft by providing safeguards to ensure the security of their most essential confidential identifying information, information which easily could be used to appropriate a person's identity.

The Bell case has national implications for employers. Arizona, California, Illinois, Texas, and other states have statutes that require an employer to restrict the use and disclosure of Social Security numbers. While not as broad as Michigan's law, they support the view that a "special relationship" exists between an employer and an employee whose data is stolen from the employer to commit identity theft.

Even in jurisdictions with no statutes restricting employers' use or disclosure of employee Social Security numbers, the tide of legislation on identity theft may be sufficient to support a finding of the necessary special relationship. The Wall Street Journal recently predicted that there will be a flood of lawsuits by both consumers and businesses because of identity theft issues.

Employers also suffer other significant costs when their employees experience identity theft. Conservative calculations based on current identity theft figures indicate that an employer with 1000 employees, who make an average of \$40,000 salary per year, should expect to incur productivity losses of more than \$600,000 per year. Identity theft also threatens enterprise security, enabling corporate espionage and fraud, and theft of hard assets and intellectual property. Large scale or frequent identity thefts also results in significant negative publicity, impacting sales, partnerships, and employee recruiting and retention.

Protection As An Employee Benefit

One solution that provides an affirmative defense against potential fines, fees, and lawsuits is to offer some sort of identity theft protection as an employee benefit. An employer can choose whether or not to pay for this benefit. The key is to make the protection available, and have a mandatory employee meeting on identity theft and the protection you are making available, similar to what most employers do for health insurance.

Employees can elect either to accept or decline to have identity theft coverage. If employees have coverage and become identity theft victims, the employer gains: The victimized employees will spend less time and money, and experience less frustration in restoring their identities. If employees decline the coverage and later claim their identities were stolen as a result of the company's actions, the employer has signed proof that they attended the presentation and declined the coverage.

Identity theft protection as an employee benefit is becoming a trend because employers are looking for ways to lower their costs. It's unique, it's hot in the marketplace, and it's relatively inexpensive.

Greg Roderick, CEO of Frontier Management, says that his employees "feel like the company's valuing them more, and it's very personal."

"I think it's a tremendous value to protect someone's name," said Matt Oros, CEO of Benelogic. "It is like a soft pillow at night that you can lay your head on and know that you're going to have an advocate."

And Donald Harris, head of the International Association for Human Resource Information Management's (IHRIM) Special Interest Group on Privacy & Security, said "Privacy is like diversity in this regard: Done the right way, each involves respecting and empowering individuals, and reaping the business benefits that this can bring, rather than acting primarily to avoid risks and legal problems."

Do Your Homework

Keep in mind that there are significant differences among the programs that are available. Many new programs are now appearing on the market to take advantage of the fear and confusion around identity theft. It is possible to spend hundreds of dollars on partial solutions that do not effectively prevent identity theft or protect the user from harm.