



Identity Theft Protection as an Employee Benefit

By Joanne Sammer, July 2008

More employers are taking steps to help employees protect themselves from becoming victims and suffering financial losses as a result of identity theft. And employers are extending help to victims trying to deal with the consequences. This move isn't completely altruistic. After all, an employee who becomes a victim of identity theft faces a range of issues that can be a major distraction for them in the workplace.

A 2007 survey conducted by the U.S. Federal Trade Commission (FTC) found that 8.3 million American adults were the victims of identity theft, including misuse of credit card and other accounts and new, fraudulent accounts opened using their personal identifying information. However, the cost of identity theft goes well beyond the value of whatever has been obtained illegally by the identity thief.

Productivity Drain

The FTC survey found that:

- **Half of identity theft victims had related out-of-pocket losses**, with 10 percent experiencing losses of \$1,200 or more.
- **To resolve identity theft-related issues**, victims spent a median of four hours resolving these problems, with 10 percent spending at least 55 hours to do so.

Identity theft goes well beyond stealing and using someone's credit card or taking out credit cards in someone's name. In some cases, criminals use the person's identity to obtain a driver's license and other documents and to commit fraud using the stolen identity. In these cases, sorting out the situation requires much more than simply canceling credit cards and opening new accounts.

There are lasting effects of identity theft, as victims are often harassed by debt collectors, denied new credit, unable to use existing credit cards, unable to get loans, have their utilities cut off, are subjected to a criminal investigation or civil suit, and have difficulties obtaining or accessing bank accounts. In some cases, identity theft victims are arrested if someone committed a crime and used the victim's identity when providing information to law enforcement officials.

From a productivity perspective, any employee who is a victim of identity theft and trying to address the resulting problems is unlikely to be fully focused on his or her work. "This can affect their workload as they are forced to spend time, at least some of which is likely to be on the job, and money to make things right," says Reginald Ball, president of iSecurity, an identity theft protection and detection company based in Washington, D.C. "If something like this happens to an employee, [he or] she is not going to be focused on her work."

Insurance Coverage

Recognizing the growing problem of identity theft, real estate investment firm Wells Real Estate Funds in Norcross, Ga., began offering company-paid identity theft insurance coverage to its employees in 2006. The program offers coverage for financial losses up to \$10,000 as well as lost wages related to identity theft, and case management for employees who are or might be victims of identity theft. For example, when an employee lost her purse recently, she contacted the insurance company's case manager to make sure she took the appropriate steps to protect her identity, according to Andy Lee, the company's vice president of employee relations and talent management.

The identity theft coverage the firm offers is cost-effective relative to the employee relations benefits the company gains. The company pays \$3,000 per year for coverage for all of its 400-plus employees and their immediate families. "It comes with minimal cost, and we get great feedback from employees," says Lee. "It represents a tremendous bang for the buck."

Other employers offer identity theft insurance as a voluntary benefit, paid for by employees (often with premiums deducted directly by payroll) but at discounted group rates that the employer negotiates with the insurance provider.

Providing Education

Companies can help employees protect themselves from identity theft in other ways. "Identity theft affects millions of people a year," says Ball. "It's important to educate employees to help them prevent this crime." Criminals are constantly finding new ways to gain access to sensitive personal information. For example, phishing schemes have traditionally used e-mail to pose as a trustworthy business in order to trick individuals into divulging personal information. More recently, however, phishing schemes have expanded to include telephone calls used for the same purpose; not all employees are aware of the new tactic. Employers can provide educational materials or hold workshops to educate employees about the basics of identity theft, about how to monitor their personal records for evidence of fraud or theft, and about what steps to take to rectify the situation. "If an employee becomes a victim of identity theft, they should immediately cancel all credit cards and bank accounts, file a police report with the local police department, place fraud alerts with the credit bureaus and monitor their credit reports for new activity or new accounts opened," says Ball.

Safeguarding Employee Information

One of the most important roles an employer can play in protecting employees from identity theft is to safeguard its HR data. "Payroll and other HR information and data about employees is a diamond that needs to be protected," says Ron Williams, CEO of Talon Companies, a security and risk management firm based in Fountain Valley, Calif. "Amateurs steal identity-related information from mailboxes. The organized ones steal data by having someone on the inside of a company or organization to gain access to data and information." Employers should remain current on developments in the federal and state legislative arenas that impact their employee data responsibilities.