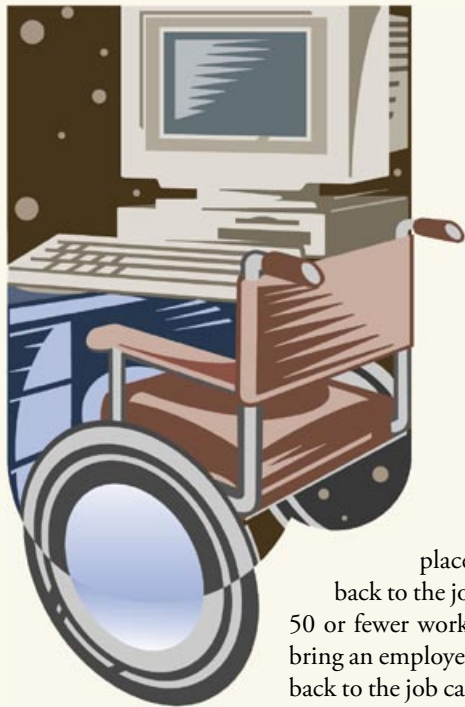


Workers' Comp



Small Employer Requirements for Workplace Modification Reimbursement

The Division of Workers' Compensation (DWC) has begun receiving reimbursement requests from employers who've modified a workplace to bring an injured employee back to the job. As a reminder, employers with 50 or fewer workers, who modify a workplace to bring an employee injured on or after Jan. 1, 2004, back to the job can be reimbursed for up to \$2,500 in expenses incurred for the modifications.

The law requires an employer to modify the workplace to qualify for reimbursement. Employers can be reimbursed up to \$2,500 for physical changes made to the workplace to accommodate a permanently disabled employee. Employers who make physical modifications that allow a

temporarily disabled employee to return to the original workplace, while they are recovering from their injury, can be reimbursed for up to \$1,250 in expenses.

In either case, the law requires the modifications be prescribed by a physician or reasonably required by restrictions set forth in a medical report. Within those parameters, reimbursement will be provided for modifications to the worksite, equipment, furniture or tools.

As a condition of reimbursement, the expenditure shall not have been paid or covered by the employer's insurer or any source of funding other than the employer. The employer must submit a *Request for Reimbursement of Accommodation Expenses* (Form DWC AD 10005) along with copies of all pertinent medical reports that contain the work restrictions being accommodated, any other documentation supporting the request and all receipts for modification expenses.

Liability

Protecting Your Company from Liability for Data Breaches

The U.S. Office for Victims of Crime estimates that identity theft has affected 27 million individuals over the past five years. Identity theft and identity fraud refer to crimes in which someone wrongfully obtains and uses another's personal information for fraudulent purposes, typically for economic gain.

For victims, ID theft is costly in terms of money, time and emotional strain. According to *Forbes.com*, "The Privacy Rights Clearinghouse estimates that victims on average spend the equivalent of 22 work days cleaning things up." (ID Theft Insurance Isn't Insurance, 5-29-03)

To commit their crimes, ID thieves use personal identifying information such as Social Security numbers, bank account or credit card numbers, telephone calling card numbers, and other valuable identifying data. So where do they get this information? *From businesses like yours.* The Privacy Rights Clearinghouse, a consumer advocacy organization in San Diego, estimates that



companies and institutions have collectively "fumbled" some 93,754,333 private records, according to a recent *New York Times* report.

ID theft costly to businesses, too.

ID theft ends up costing not only the victims, but the organizations where the information breach occurred. Risk exposures include:

★ **Liability.** According to PLUS, the Professional Liability Underwriting Society, the number of privacy lawsuits has increased 300 percent in the last 10 years.

★ **Fines.** Many federal laws govern privacy and call for penalties when an organization fails to take appropriate steps to protect individuals' personal identifying information.

★ **Notification costs.** At time of publication, 29 states had laws requiring businesses and

nonprofits to notify their clients when their personal information is breached. These states include: Arkansas, Arizona, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Kansas, Louisiana, Maine, Minnesota, Montana, Nebraska, Nevada, New

Jersey, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Rhode Island, Tennessee, Texas, Washington and Wisconsin. Laws will take effect in Kansas, New Hampshire and Utah on January 1, 2007. Standards for notification vary by state—stricter standards, such as California's, call for notification for any breach. Less-strict standards require notification only if a risk of identity theft exists. For details on state laws, see the State PIRGs (Public Research Interest Groups) site at www.pirg.org/consumer/credit/statelaws.htm.

So, what does notifying customers cost? A survey by the Ponemon Institute found that each lost record costs companies an average of \$140, for a total of \$5 million in direct costs per incident.

✳ **Public relations costs.** A breach of customer information can damage an organization's reputation. Another study by the Ponemon Institute found that, of the 23 million U.S. adults who have been notified of a breach of their personal data, approximately 20 percent terminated their accounts and another 40 percent were considering it. Adverse publicity from the breach will likely impact sales as well.

How do you minimize the risk of data breaches?

To protect your business from liability for data breaches, familiarize yourself with privacy laws. Federal laws governing the security of private consumer information include:

- ✳ **Family Educational Rights and Privacy Act of 1974 (FERPA):** Applies to educational institutions and agencies that receive federal funding.
- ✳ **Fair Credit Reporting Act (FCRA):** Applies to credit reporting agencies and credit bureaus.
- ✳ **Financial Services Modernization Act (Gramm-Leach-Bliley):** Applies to financial institutions.
- ✳ **Video Privacy Protection Act of 1998:** Applies to video rental or sales outlets.

✳ **Health Insurance Portability and Accountability Act of 1996 (HIPAA):** Applies to health plans (including self-insured employers), health care clearinghouses and providers.

✳ **Children's Online Privacy Protection Act (COPPA):** Applies to almost all commercial Web sites and online services, requiring them to obtain parental consent before collecting personal information from children under 13.

✳ **Fair and Accurate Credit Transactions Act:** Applies to any business or individual who uses consumer information for business purposes. The Act requires consumer information to be disposed of properly to prevent "unauthorized access."

Action steps you can take to minimize your exposures include:

- ✳ Ensure your IT department uses the latest technology to secure data and networks, and prevent unauthorized personnel from accessing your systems.
- ✳ Avoid using employee Social Security numbers for identity numbers and limit access to employees' private information—including information on medical conditions, claims and disabilities—to a need-to-know basis. Ensure that this information is stored on secure systems, and that those with access to it log off their computers when away from their desks.
- ✳ Dispose of any records containing personal data properly. Shred printed records before discarding. And when disposing of any electronic media (including hard drives), either destroy the media or reformat it—when you simply "erase" data, it just gets overwritten and can be recreated.
- ✳ Consider buying one of the new identity theft policies for businesses. These policies protect your firm from liability losses when your data is stolen or used by identity thieves. Policies cover direct expenses, such as defense costs, legal damages, fines, regulatory actions and notification costs. Some policies also cover services that protect or help restore your reputation, including public relations counsel and assistance for victims. Group policies that protect your employees from the costs of identity theft are available as well. □