
Privacy Rights: Protecting Your Employees From Identity Theft

In the 1950s, your major concern in terms of employee theft was office supplies. A few missing pens and paperclips were the price for hiring help. However, things have changed dramatically. Today, many workplace thieves are stealing a lot more than notepads; they are stealing co-workers' identities and you may be the one held liable!

Since an employment file includes a great deal of personal information such as Social Security number, home address and date of birth, it is a gold mine for a thief. The Human Resources department hosting the files may be part of the problem.

The Department of Justice defines identity theft as a type of crime wherein one wrongfully obtains and uses another's personal data in a fraudulent or deceptive manner, typically for economic gain. It is estimated that over 100,000 confirmed identity theft cases occur each year in the United States. Moreover, the average financial loss for the victim is over \$50,000.

Since no raw data exists as to what percentage of identity theft occurs in the workplace, employers have not been clued into this "pre-epidemic" disaster. And, regardless of whether personnel files are stored manually or electronically, the opportunity for theft is there for the taking.

As a manager, you learn to trust your employees. So who could be a hidden thief? The most likely culprits are the

transient and disgruntled workers. Some are small time thieves going at it alone, and some are part of highly organized and efficient organizations.

The most likely result of identity theft is use of the information to order credit cards, charge the maximum on all, and sell the proceeds illegally. By the time the employee victim receives the credit card statement the thief is long gone and someone is liable for thousands of dollars.

When can you be held liable for identity theft? First and foremost, if the employee can show that as an employer you have demonstrated a disregard for proper protection of personal information, you may be open to civil liability.

The following are three keys to protect your employees from identity theft and in turn, help shield yourself from liability:

1. **Secure storage of personal data.** While no mechanism for securing personal data, electronic or other, is fully failsafe reasonable precautions must be taken. Leaving personal files in an open and totally accessible area may put you on the hook for the loss.
2. **Background Checks.** Personnel with access to personal data should be subject to background screening as a condition of employment. Just as you would not want a CFO with an embezzlement background, you don't want an HR director with a fraud conviction.
3. **Access to personnel files.** Persons with access to personnel files, such as

HR staff, should be required to sign a confidentiality agreement.

Furthermore, all employees should be made aware of the serious consequences of appropriating another's personal information for illegal use.

Finally, as a hospitality institution, you carry the same responsibility to your guests. For example, a hotel may require a person's name, address, and credit card number in order to reserve a room. You have a duty to protect this information as you have a duty to protect your

employees' information.

In sum, instituting risk prevention methods to insure the safety of personal data for both guests and employees may save you hundreds of thousands of dollars in the end. When the average victim loses \$50,000 per incident, imagine the potential liability you risk without instituting proper precautions.

As some states differ in the manner such liability is assigned, it is best to contact local counsel for advice on what is best in instituting your loss prevention system.

#

For additional information, contact Joe Dworak, joseph.dworak@berliner.com, or Christine Long, christine.long@berliner.com, Berliner Cohen attorneys, or 408.286.5800.

Berliner Cohen's experienced employment law attorneys advise and represent employers and managers on a full range of legal issues affecting the workplace, including harassment and discrimination, unfair competition and trade secrets, wrongful discharge, wage and hour issues, and labor disputes. Berliner Cohen is one of the largest and oldest law firms in San Jose serving the business and regulatory needs of private business and public agencies in Northern California. For 40 years, the Firm has developed the special expertise required by a diverse client base consisting of nationally recognized business interests and a number of Silicon Valley's largest national and multinational corporations, new ventures, leading real estate developers and brokerages, cutting-edge technology companies, healthcare and other service providers, banking and financial institutions, municipalities, public agencies and individuals. Berliner Cohen also meets the growing demands of the San Joaquin Valley with its expanding office in Merced.