

Identity Theft: Growing Concern for Employers

Comedian Jay London once joked “I don’t need to worry about identity theft because no one wants to be me.” Unfortunately, identity theft is no laughing matter. It has rapidly become the Nation’s top consumer fraud problem. Bank of America, CitiBank, LexisNexis and ChoicePoint are just a sampling of corporate giants that have been the source of privacy leaks. In 2004, there were 246,570 complaints of identity theft, of which 32,954 or 13% stemmed from the workplace. Employment-related identity theft has more than doubled since 2002.

Any victim of identity theft can attest to the seriousness of the crime. Studies indicate that victims spend on average over 270 hours researching and tracking the crime, 23 months correcting credit reports and incur about \$800 of out-of-pocket expenses attempting to clean their credit.

The Hospitality sector is far from immune as identity theft poses significant liability risks for employers. Human resource departments are often the repository of significant amounts of personal data including social security numbers, names, addresses, birth dates, payroll tax records, and medical records. Anyone who has access to this information has the means to carry out identity theft. Thus, it is critical that companies take measures to protect such information. The consequences of not doing so are real. In one case, a California pharmaceutical company was forced to settle a lawsuit brought by some of its former employees who were victims of identity theft. In that case, an employee found a box of personnel records and used the information to open 20 cell phone accounts, rent three apartments and open more than 25 credit card accounts, which were used to purchase \$100,000 of merchandise. Earlier this year, a Michigan state appellate court affirmed a \$275,000 jury verdict against a union for failing to protect the social security numbers of several of its members.

While it is impossible to prevent identity theft from ever incurring, employers can minimize the possibility of such crime and limit their legal liability by taking preventative steps to protect employee information including the following:

1. Develop a company policy that ensures the confidentiality of social security numbers and other data, limits who has access to information, describes how to properly dispose of records and establishes penalties for violation of the policy.
2. If records are maintained electronically, develop reasonable controls to ensure the integrity, accuracy and reliability of the storage system including controls to prevent and detect unauthorized access to the information.
3. Keep employee data and personal information about vendors locked.
4. Do not let employees take home employee records and personnel information.
5. Do not use social security numbers as a form of employee identification.
6. Shred all discarded employee information.

7. Conduct background checks and criminal checks of employees who will have access to personnel data.
8. Implement proper security control devices to prevent e-mailing of personnel information.
9. Limit the use of temporary workers to the extent possible. Do not allow temporary workers access to confidential information.
10. Have employees execute non-disclosure and confidentiality agreements.

In sum, employers must be vigilant in protecting personal information. By creating a company culture that values the protection of its employee information, employers will go a long way in combating the identity theft epidemic.

By Kenneth N. Winkler. Nothing herein is intended to constitute a legal opinion or advice. If you have particular questions or concerns as to the issues discussed in this article, please contact Kenneth Winkler at Berman Fink Van horn P.C.; (404)261-7711 to assist you.