

QUICK JUMP:

Make a selection

NAVIGATION

- Career Opportunities
- Events Schedule
- Attorneys
- Offices
- Archives
- About BS&K
- Contact BS&K
- Home

INDUSTRIES

PRACTICES

Information Memos, Articles, White Papers

Securing Employment Records Aids In The Prevention Of Identity Theft (12/05)

By Nicholas J. D'Ambrosio, Jr., *Capital District Business Review*, December 2-8, 2005

The growing problem of identity theft has garnered a lot of attention in the past few years and with good reason--identity theft is one of the fastest-growing crimes in the United States.

Last year, New York state had, per person, the seventh highest incident rate of identity theft nationally. Of concern to employers, employment records were one of the most popular sources of personal information for identity theft. In fact, just a few years ago, Credit bureau TransUnion reported that employer records are the No. 1 source of information used in identity theft.

There are several reasons that employers make such good sources for personal information. First, employers obtain and maintain a great deal of information about employees and applicants, such as names, addresses, dates of birth and Social Security numbers.

Frequently, many employees have access to personal information maintained by employers, either in paper files or on the computer. Where the employer maintains computer records, personal information can often be stolen quickly and discretely.

As employer records are such a gold mine for identity thieves, some individuals have actually planted themselves with an employer specifically to steal employees' personal information.

Stolen employment records are a human relations nightmare. Theft of employees' personal information will generally lead to adverse publicity for the employer, problems with employee morale and lost time and reduced productivity while employees try to correct ruined credit ratings.

If a breach of security does occur and personal information is stolen, the employer should promptly inform employees and applicants whose information has been stolen. In giving notice of the theft, the employer provides an opportunity for those individuals to take preventative measures to protect their credit.

Additionally, effective Dec. 7, New York state law requires employers to notify any individual whose personal information is acquired by an unauthorized party during a breach of a computer system. The employer may make this disclosure by written notice; electronic notice, when made with the consent of the person to whom the disclosure must be made; or telephone.

The employer must also notify the state Attorney General, the Consumer Protection Board, and the state Office of Cyber Security and Critical Infrastructure Coordination. The statute provides specific requirements for the content of the notice and proof that the notices were given.

Fortunately, there are several steps that an employer can take to reduce the

SEARCH:



potential for theft of employees' personal information:

- Develop written policies and procedures for collecting, maintaining and sharing personal employee information.
- Keep personnel files in a locked cabinet and limit the number of employees who have access to cabinet.
- Avoid giving temporary employees access to personal information.
- Conduct background checks on anyone who will have access to personal information.
- Train individuals who will handle personal information.
- Revoke access to personal information immediately upon terminating an employee.
- Create a log for monitoring access to personnel files.
- Avoid using personal information where another identifier, such as an employee number, would suffice.
- Require employees to change passwords regularly.
- Shred documents containing personal information once those documents are no longer needed.
- Ensure that all storage sites (on-site or off-site) are secure.
- Perform periodic self-audits to ensure that procedures are being followed and information is secure.

In addition to taking these steps, federal law requires employers to take reasonable measures to protect against unauthorized access to or use of the information obtained by a reports obtained from consumer reporting agencies (i.e., third parties who are in the business of providing consumer reports, such as a private investigator or other company in the business of conducting background checks) and any information derived from such reports.

To comply with this requirement, employers must destroy documents with information from a consumer report by (1) burning, pulverizing, or shredding papers containing this information, (2) destroying or erasing any electronic media containing this information, or (3) contracting with an entity in the business of record destruction to dispose of material identified as consumer information.

Taking preventive steps to prevent the unauthorized disclosure of personal information will go a long way to protecting your employees from identity theft and your company from a negligence claim.

Note: This article first appeared in the December 2-8, 2005 edition of the *Capital District Business Review*, which is published weekly in Albany, New York.

[Return to Previous Page](#) | [Back To Top](#) | [Join Our Electronic Mailing List](#)

[Privacy Policy](#)

[Disclaimer / Client Rights](#)

[Site Map](#)

• ©2003 BS&K All Rights Reserved

[BS&K Home](#)